

LL

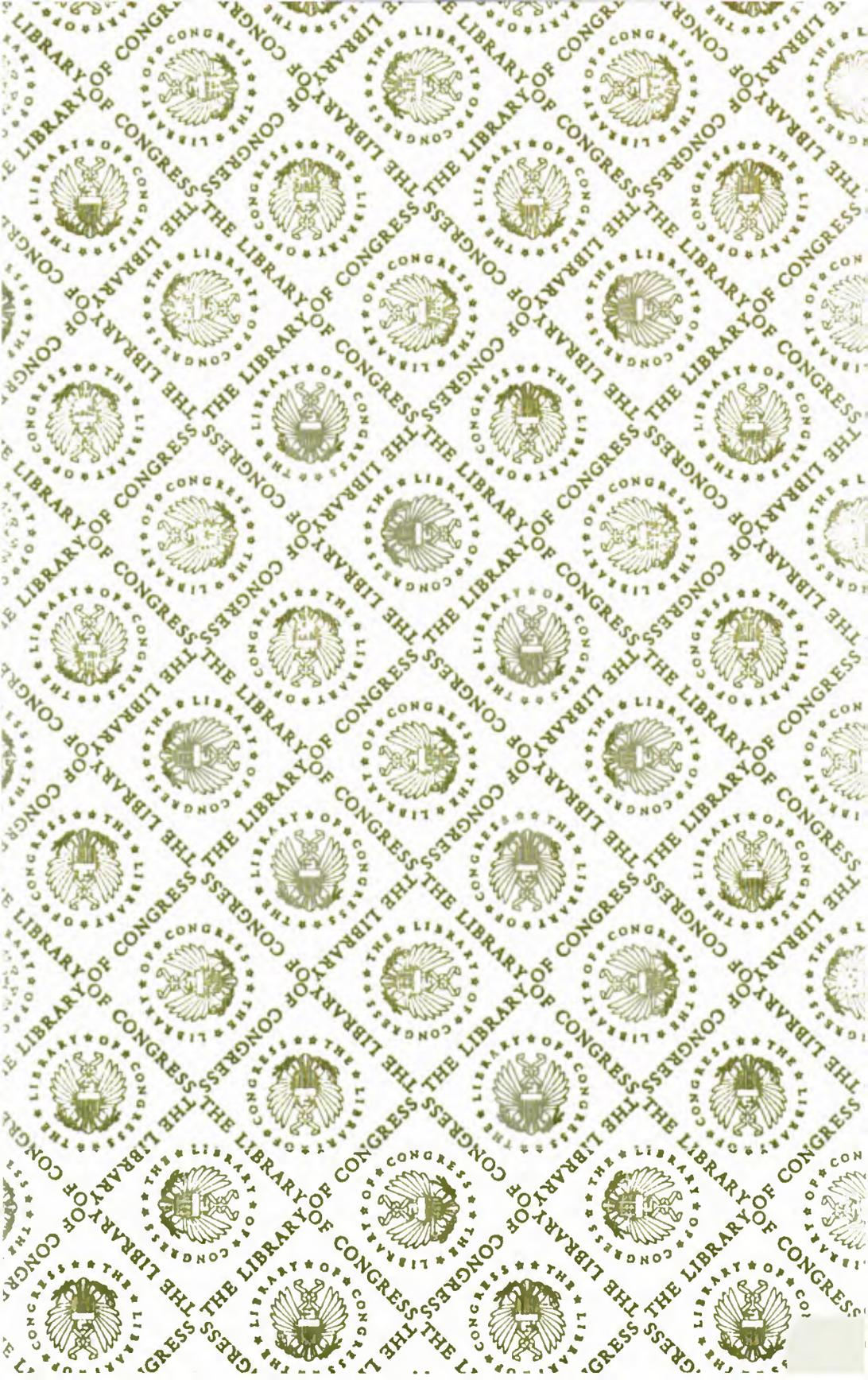
KF 27

.J858

1997f

Copy 1







UNITED STATES CONGRESS, HOUSE, COMMITTEE ON THE JUDICIARY,  
SUBCOMMITTEE ON CRIME.

# IMPLEMENTATION OF THE COMMUNICATIONS AS- SISTANCE FOR LAW ENFORCEMENT ACT OF 1994

---

---

**HEARING**

BEFORE THE  
SUBCOMMITTEE ON CRIME  
OF THE  
COMMITTEE ON THE JUDICIARY  
HOUSE OF REPRESENTATIVES  
ONE HUNDRED FIFTH CONGRESS  
FIRST SESSION



OCTOBER 23, 1997

**Serial No. 136**



Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE  
WASHINGTON : 2000

61-763

---

For sale by the U.S. Government Printing Office  
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402  
ISBN 0-16-060074-X

## COMMITTEE ON THE JUDICIARY

HENRY J. HYDE, Illinois, *Chairman*

F. JAMES SENSENBRENNER, Jr.,  
Wisconsin

BILL McCOLLUM, Florida

GEORGE W. GEKAS, Pennsylvania

HOWARD COBLE, North Carolina

LAMAR SMITH, Texas

STEVEN SCHIFF, New Mexico

ELTON GALLEGLY, California

CHARLES T. CANADY, Florida

BOB INGLIS, South Carolina

BOB GOODLATTE, Virginia

STEPHEN E. BUYER, Indiana

SONNY BONO, California

ED BRYANT, Tennessee

STEVE CHABOT, Ohio

BOB BARR, Georgia

WILLIAM L. JENKINS, Tennessee

ASA HUTCHINSON, Arkansas

EDWARD A. PEASE, Indiana

CHRISTOPHER B. CANNON, Utah

JOHN CONYERS, Jr., Michigan

BARNEY FRANK, Massachusetts

CHARLES E. SCHUMER, New York

HOWARD L. BERMAN, California

RICK BOUCHER, Virginia

JERROLD NADLER, New York

ROBERT C. SCOTT, Virginia

MELVIN L. WATT, North Carolina

ZOE LOFGREN, California

SHEILA JACKSON LEE, Texas

MAXINE WATERS, California

MARTIN T. MEEHAN, Massachusetts

WILLIAM D. DELAHUNT, Massachusetts

ROBERT WEXLER, Florida

STEVEN R. ROTHMAN, New Jersey

THOMAS E. MOONEY, *Chief of Staff-General Counsel*

JULIAN EPSTEIN, *Minority Staff Director*

## SUBCOMMITTEE ON CRIME

BILL McCOLLUM, Florida, *Chairman*

STEVEN SCHIFF, New Mexico

STEPHEN E. BUYER, Indiana

STEVE CHABOT, Ohio

BOB BARR, Georgia

ASA HUTCHINSON, Arkansas

GEORGE W. GEKAS, Pennsylvania

HOWARD COBLE, North Carolina

CHARLES E. SCHUMER, New York

SHEILA JACKSON LEE, Texas

MARTIN T. MEEHAN, Massachusetts

ROBERT WEXLER, Florida

STEVEN R. ROTHMAN, New Jersey

PAUL J. McNULTY, *Chief Counsel*

GLENN R. SCHMITT, *Counsel*

DANIEL J. BRYANT, *Counsel*

NICOLE R. NASON, *Counsel*

DAVID YASSKY, *Minority Counsel*

#11963618

LC Control Number



00 325544

KF27  
J858  
1997F  
COPY 1  
LL

## CONTENTS

### HEARING DATE

October 23, 1997 .....	Page 1
------------------------	-----------

### OPENING STATEMENT

McCollum, Hon. Bill, a Representative in Congress from the State of Florida, and chairman, Subcommittee on Crime .....	1
---	---

### WITNESSES

Allen, Edward L., Chief, Electronic Surveillance Technology Section, Federal Bureau of Investigation .....	97
Dempsey, James X., Senior Staff Counsel, Center for Democracy and Tech- nology .....	65
Flanigan, Matthew F., President, Telecommunications Industry Association ...	47
Kitchen, Jay, President, Personal Communications Industry Association .....	31
Neel, Roy M., President, U.S. Telephone Association .....	37
Warren, H. Michael, Chief, CALEA Implementation Section, Federal Bureau of Investigation .....	97
Wheeler, Thomas E., President, Cellular Telecommunications Industry Asso- ciation .....	5

### LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

Dempsey, James X., Senior Staff Counsel, Center for Democracy and Tech- nology: Prepared statement .....	69
Flanigan, Matthew F., President, Telecommunications Industry Association: Prepared statement .....	50
Kitchen, Jay, President, Personal Communications Industry Association: Pre- pared statement .....	33
Neel, Roy M., President, U.S. Telephone Association: Prepared statement .....	39
Warren, H. Michael, Chief, CALEA Implementation Section, Federal Bureau of Investigation: Prepared statement .....	99
Wheeler, Thomas E., President, Cellular Telecommunications Industry Asso- ciation: Prepared statement .....	8



# **IMPLEMENTATION OF THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT OF 1994**

**THURSDAY, OCTOBER 23, 1997**

**HOUSE OF REPRESENTATIVES,  
SUBCOMMITTEE ON CRIME  
COMMITTEE ON THE JUDICIARY,  
*Washington, DC.***

The subcommittee met, pursuant to notice, at 10:05 a.m., in Room 2237, Rayburn House Office Building, Hon. Bill McCollum [chairman of the subcommittee] presiding.

Present: Representatives Bill McCollum, Stephen E. Buyer, Steve Chabot, Bob Barr, Asa Hutchinson, Martin T. Meehan, and Robert Wexler.

Staff present: Paul J. McNulty, Chief Counsel; Glenn R. Schmitt, Counsel; Kara Norris, Staff Assistant, and David Yassky, Minority Counsel.

## **OPENING STATEMENT OF CHAIRMAN McCOLLUM**

Mr. McCOLLUM [presiding]. The subcommittee will come to order.

We have a significant hearing this morning and so, with Mr. Meehan's indulgence, who's here with us, and I'm sure others will wander in, I'm going to get started with this hearing.

I have an opening statement I'd like to make because the subject is complex, I think it's important, and I'd like to at least lay the predicate for our first panel.

Today, the subcommittee conducts a hearing on a subject of vital importance to the enforcement of criminal laws and the prevention of crime. This hearing concerns the implementation of the Communications Assistance for Law Enforcement Act, better known as CALEA. This act passed in 1994 and was designed to preserve the government's ability, pursuant to court order, to intercept communications involving advanced technologies while protecting the privacy of communications without impeding the introduction of new technologies into the market. The act was to be fully implemented by next year. It appears now that this may not occur, and a primary purpose of this hearing is to find out why.

The act requires telecommunications carriers to do four things by October 1998. First, carriers are expected to enable the Government to intercept all wire and electronic communications within a carrier's service area concurrently with their transmission. Second, carriers are required to enable the Government to access call iden-

tifying information that is reasonably available to the carrier before, during, or immediately after the transmission of a communication. Third, carriers are required to provide intercepted communications and call identifying information to a location selected by the Government. Finally, the act requires carriers to perform these interceptions unobtrusively, without interfering with a subscriber's service, and in a manner that protects the privacy and security of information not authorized to be intercepted.

As important as what CALEA requires is what it does not provide. The act states that law enforcement is not authorized to require any specific design of equipment, facilities, or services. The Government also cannot prohibit the adoption of equipment, facilities, or services by any provider or manufacturer.

The act requires that telecommunications carriers have the functional capability of doing the things that CALEA requires by October, 1998. The various telecommunications industry associations have informed the subcommittee that this is not possible because industry and law enforcement, principally represented by the FBI, have been unable to agree upon the meaning of CALEA. More clearly stated, the two sides have been unable to agree exactly as to what law enforcement is entitled to receive and the manner in which telecommunications carriers are required to provide it. This hearing is to provide both sides with a chance to explain their positions concerning this dispute.

CALEA required the Attorney General to specify the maximum number of simultaneous communication interceptions, pen registers, and trap-and-trace devices that the Attorney General estimated the Government might conduct on and after October, 1998. The Attorney General was to have provided this information in final form to carriers, and to the public, by October, 1995. So far, the Attorney General has failed to do this. One of the purposes of this hearing is to determine why the Attorney General has failed to comply with the act's requirement in this regard.

The drafters of CALEA recognized that equipment deployed prior to its enactment might not be functionally capable of complying with the act's requirements. The act provides that the Attorney General may specify systems to be retrofitted in order to have CALEA capability.

The act also requires, however, that the Government pay for the reasonable costs associated with making the necessary modifications. Because the industry and the FBI continue to dispute the meaning of CALEA, the industry asserts that it is unfair to expect that any of the equipment placed into service since CALEA was enacted will comply with the act. Accordingly, they have asked the subcommittee to consider modifying CALEA to make the Attorney General's power to demand this equipment be retrofitted to also be conditional upon the Government's agreement to pay for these modifications.

I am also very much aware that since CALEA was enacted, a significant number of new companies have entered the wireless telecommunications industry. A number of these companies operate using technology that was not even in use when CALEA was enacted in 1994. Most, if not all, of the equipment installed by these companies was installed after CALEA was enacted, yet was devel-

oped before or during the ongoing dispute between the two sides as to what CALEA means. These companies also assert that their equipment should also be eligible for the retrofit monies and should not be required to comply with CALEA unless the Government pays for those modifications.

Finally, I know that a number of privacy groups assert that the demands the FBI is making on the telecommunications industry go beyond CALEA's requirements, so far in fact, that they impinge upon the constitutionally protected privacy rights of all citizens. This is an important issue and I expect the issue to be addressed during today's hearing.

I believe it's fair to say that when CALEA was enacted in 1994, no one expected that today, 3 years later, CALEA would still be not implemented. Today's hearing is not to assess blame for this, but to determine what can be done to implement CALEA as soon as possible. All parties should bear in mind that the purpose of the act was to help law enforcement protect the citizens of our country. Each day that the dispute over CALEA continues is another day where this protection is not in place, making it more likely that criminals will succeed in preying upon the citizens of our country.

The stalemate must be broken, and soon. I hope that it will be resolved through cooperation and compromise of all the parties in the near future. If this is not the case, however, I intend to involve this subcommittee, the authorizing subcommittee for this legislation, to end the impasse. The safety of our citizenry depends upon it. Any further delay is a disservice to them.

Mr. Meehan, would you like to make any opening comments?

Mr. MEEHAN. I would, thank you, Mr. Chairman, and I do want to commend you for holding this hearing, although I must say that I am very disappointed at the circumstances that necessitate it. But clearly, our high hopes for CALEA upon its enactment in 1994 seem to be in serious jeopardy. Industry and law enforcement have failed to reach an agreement on capability and capacity standards. Not a single dime of the Telecommunications Carrier Compliance Fund has been spent to date. And industry witnesses will tell us that even in the best-case scenario, the industry will not be able to meet its current statutory deadline for compliance with CALEA's capability requirements.

I don't believe that there is a singular villain in this CALEA controversy solely responsible for the current impasse. Rather, this is a story of well-intentioned parties, skirmishing over the meaning of a murky statute with enormous consequences at stake. Indeed, the law enforcement must have the capability and capacity to employ wiretaps and pen registers against criminals using increasingly sophisticated telecommunications technology. But it would be entirely unreasonable to demand that the telecommunications industry finance the necessary equipment upgrades, without fair and equitable reimbursement from the Federal Government.

I hope that today's hearing will not serve to entrench current positions or inflames animosities, but rather to spur ongoing negotiations and resolve this unfortunate controversy. Indeed, I understand that the negotiations have recently made significant progress due to greater involvement on the part of main Justice and the concerned Members of Congress.

Now, members of this subcommittee stand ready to take whatever action is necessary to bring about a resolution to this matter and thereby speed the deployment—speed up the deployment of CALEA complaint technology.

Thank you very much, again, Mr. Chairman, and I yield back the balance of my time. I look forward to working with you on this issue.

Mr. MCCOLLUM. Thank you. Mr. Chabot, do you have any opening remarks?

Mr. CHABOT. Mr. Chairman, in order to save time so that we can get right on to the testimony from the witnesses, I'll not make an opening statement at this time. Thank you for holding this hearing.

Mr. MCCOLLUM. Thank you. Mr. Hutchinson?

Mr. HUTCHINSON. I'll save my remarks for later, Mr. Chairman. I do thank you for holding this hearing. I think you've correctly outlined the issues and I look forward to the testimony.

Mr. MCCOLLUM. Thank you.

I'll introduce, then, our first panel. They've fortunately been seated already, which is good for us; it saves a little time.

Thomas E. Wheeler is president and CEO of the Cellular Telecommunications Industry Association. Mr. Wheeler has been involved in telecommunications policy and technology for twenty years and has founded or helped start multiple companies offering cable, wireless, and video communications services both domestically and internationally. He served as president of the National Cable Television Association from 1979 to 1984. He's a member of the Board of Trustees at the Kennedy Center for the Performing Arts, the Vincent Lombardi Foundation, and the United States Capital Historical Society. Mr. Wheeler is a graduate of The Ohio State University.

Jay Kitchen is president of the Personal Communications Industry Association, a trade association for those telecommunications companies which use the PCS technology to transmit wireless telecommunications. Prior to assuming his present position, Mr. Kitchen spent 17 years at the National Association for Business and Educational Radio first, as vice president, then as president. Prior to joining NABER, Mr. Kitchen served for 9 years at the Federal Communications Commission as assistant to two FCC Commissioners. He holds degrees in electrical engineering from Virginia Polytechnic Institute.

Matthew J. Flanigan is president of the Telecommunications Industry Association, the trade association representing over 600 large and small telecommunications equipment manufacturers. He began his career in 1964 with the Cognotronics Corporation, retiring as its president and chief officer in 1994. Or I should say 1964—I didn't say that right. You began a little bit earlier than I had put you down as being there, Mr. Flanigan.

He is a member of the Board of Governors of the Electronic Industries Association and also a member of the Network Reliability and Interoperability Council of the Federal Communications Commission.

I skipped over Mr. Neel. I didn't mean to do that. Roy M. Neel is president of the United States Telephone Association, the trade association that represents companies providing local telephone

service. Prior to joining USTA in 1994, Mr. Neel was Deputy Chief of Staff to President Clinton, coordinating all policy, political and communications activities conducted by assistants to the President.

Prior to working at the White House, he was Legislative Director and later Chief of Staff to Vice President Gore while he was a member of the House and Senate. He's also a member of the Board of Directors of Amtrak. Mr. Neel received his undergraduate degree at Vanderbilt University and his Master of Public Administration from Harvard University. I might add that we could certainly use Mr. Neel's help with the Amtrak legislation right now, but that's a separate issue. [Laughter.]

James X. Dempsey is senior staff counsel at the Center for Democracy and Technology. CDT is a non-profit, public interest organization working to develop and implement public policies to protect individual liberties in the new digital media. From 1995 to 1996, Mr. Dempsey was Deputy Director of the Center for National Security Studies and Special Counsel to the National Security Archive, a non-governmental organization that uses Freedom of Information Act to gain declassification of documents on U.S. Foreign Policy.

From 1985 to 1994, Mr. Dempsey was Assistant Counsel to the House Judiciary Committee on Civil and Constitutional Rights. During that time, he helped to write the statute under consideration today. He's a graduate of Yale College and Harvard Law School and some of us are particularly pleased he's here today because he did help write the statute and we need you to help us get out from under all of this.

So the combination of this panel is very good and very powerful and I think we can look forward to solid testimony. What I'd like to do is to state for the record without objection that the written testimony of each of these witnesses will be admitted to the record, and, as I hear no objection, it is so ordered. I would encourage you, because we do have a lengthy hearing today, to summarize your testimony—five minutes, hopefully you can come close to that—if it's a little bit more, I'm not going to be as strong as Mr. Hyde, but I—in gaveling you down or something, but I would hope that we would not have too—too long a testimony.

Now we're going to go from left—my left to right, starting with Mr. Wheeler and then just down the line. Mr. Wheeler, please tell us what you're thinking.

#### **STATEMENT OF THOMAS E. WHEELER, PRESIDENT, CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION**

Mr. WHEELER. Thank you very much, Mr. Chairman. And thank you for your introductory comments which did a terrific job of putting this whole thing in context and laying out the issues before us today.

I'm proud to be here to represent the wireless industry, both cellular and PCS providers, because it was at this very table, I think, that Roy Neel, and Director Freeh and I sat just a few years ago before this same subcommittee and together endorsed the passage of this legislation as an important step to move telecommunications into the digital age.

Let me put up a chart here to show you something real quickly. This is why we supported this legislation. There—the bar chart shows you the total number of taps that were Title 3 taps in 1993 and 1996 and that of those taps about a third of the 1996 number were done on wireless phones. Comparative wiretap statistics means that, with the next chart up there, that we are actually doing a greater per subscriber line accommodation of law enforcement's wishes on wireless than has traditionally been the case in wire line. Because at the time that there were 33 percent of the taps on wireless, we only had 16 percent of the subscribers in America. Comparative wiretap statistics 1996, we are today facilitating wiretaps and will continue to facilitate lawful wiretaps.

The purpose of CALEA, as you indicated, was to update the law to new technology. And as pre-SP3580 call-forwarding, the committee said in its report—that quote which is up there at the top that I won't read to you, but the concept was how do you deal with new technologies such as call-forwarding which allows someone, when that phone at the bottom is being lawfully tapped, to avoid the tap by having the call forwarded to another phone? Pre-SP3580 call forwarding CALEA was designed to solve that problem. What the industry has done in the standard which has been put forward by the industry—so-called Standard 3580—is to come up with a plan that accomplishes exactly what this committee asked for, and that is to make sure that the new capabilities of networks cannot be used to thwart a tap.

Metaphorically, I think what we're talking about here is how do we move from a propeller-driven airplane to a jet airplane? The problem has been that law enforcement has decided they want to build the Apollo program and send a man to the moon. And in the process, they have used CALEA as a vehicle to expand wiretap authority, which clearly, as the committee report states, was not the goal of the legislation, and also to play a shell game with the money to lay off the cost of the Apollo program on the industry, which, again, as you indicated in your opening remarks, was not the intent of Congress.

The Congress asked the industry—Congress directed the industry—to develop a standard which would solve the kinds of problems we were talking about here. That standard has been developed. The industry met 1 week every month for 2½ years, and came up with this rather voluminous document that lays out and complies with the requirements of CALEA.

We thought it was going to be a rather quick process to complete the CALEA capabilities standard. Unfortunately, as this document neared completion, a new document appeared on the table. This is called "The Electronic Surveillance Document" which was put forth by the FBI and which really amounted to rolling a hand grenade underneath the table of the standards process. Because this was presented on the basis of "take it, or else," that this is what FB—this is what law enforcement wants and if you don't agree with this, we will find you in non-compliance and there are \$10,000 a day per instance penalties as we are authorized by CALEA.

On the day that this document was presented as the standard was nearing completion, the October 1998 compliance date in CALEA and the January 1995 cost-reimbursement dates became

unachievable. Since then, unfortunately, things have only become worse. The standard was developed, as I said, here it is. It was put out for ballot and in a campaign orchestrated by the FBI it was voted down.

The industry group came back again and rehashed some of the issues, came out with another document that is now out for industry ballot literally as we speak. We've been told by the FBI that they won't approve that, either.

So CALEA is in a trap set by middle-level engineers at the FBI, if you will, where, if one was suspicious, one could say that perhaps the name of the game is to stall the standard until the industry's back is up against this immovable October 1998 date and then, staring down the barrel of that gun, the industry might give into the FBI's demands and provide features that are outside the scope of CALEA.

And secondly, there has been an activity to hide the costs of what this document would cost by preying on new entrants, such as the PCS carriers who weren't even in existence when CALEA was enacted. That if—if a carrier puts in effect an FCC-mandated upgrade to its switch, it immediately disqualifies him for reimbursement.

So you have one arm of the Government over here saying "make these improvements to the switch," and the other arm of the Government saying "Oops, that now means that you can't pay for it." And that's the way the Apollo program gets paid for because the industry then steps up and pays for it rather than the 500 million dollars that this committee has authorized.

There is an additional issue in here which you raised, Mr. Chairman, and that is the capacity standards. The Congress said that the FBI should develop capacity standards, how many taps should be done simultaneously? We're talking here about capability, what do those taps do? But the capacity standards were the responsibility of the FBI and this committee said those standards will be established within 1 year of enactment, October 1995. We are now told that we will see them in January 1998. You can't develop a capability standard until you know the capacity that's required. And it certainly isn't efficient to start writing lines of code until you know both parts of the equation. We could start the work on capabilities, Mr. Chairman, but you got to go back and do it over after the capacity requirements become known and it's doubly expensive for the taxpayers and for the industry and doesn't make any sense.

But the fact that this delay has taken place by the FBI, is now 3 years behind in coming up with the capacity requirements. This means that it will clearly be impossible for industry to meet the October 1998 date because we're not going to know what the Government's capacity requirements are until 10 months before the deadline. And you can't build software that fast.

So in conclusion, Mr. Chairman, the situation we find ourselves in today is: (1) the wireless industry is supporting lawful taps; (2) that we don't know the capacity to build into our switches; (3) that we developed a standard which is a hundred percent compliant with CALEA, but we can't put it into effect because of the roadblocks from the FBI, and (4) that the new competitors, PCS, are hit with a double-whammy because if they were to get to market,

they had to buy equipment which was per se non-compliant, yet they can't get reimbursed for the upgrade of that equipment.

CALEA needs to be rescued from the trap that it is in. In 1 year and 2 days from today, 367 days from today, the October 1998 deadline will be upon us. You can't write code that fast, Mr. Chairman, and we hope that this committee will extend the October 1998 deadline, as well as eliminate the January 1995 grandfather date. Thank you very much.

[The prepared statement of Mr. Wheeler follows:]

PREPARED STATEMENT OF THOMAS E. WHEELER, PRESIDENT, CELLULAR  
TELECOMMUNICATIONS INDUSTRY ASSOCIATION

SUMMARY

In 1994, as president of CTIA, I joined FBI Director Freeh "with a gentleman's handshake" to support CALEA as a balanced bill that would ensure law enforcement's ability to conduct authorized wiretaps in the future without impeding the introduction of new technologies, features and services along the way. CALEA was the codification of the long-standing spirit of cooperation that has always existed between the telecommunications industry and law enforcement in the conduct of lawfully authorized surveillance.

The timely and cost-effective implementation of CALEA is of the utmost importance to CTIA's membership. Wireless wiretaps accounted for less than 25% of all wiretaps conducted in 1993. The wireless share of wiretaps has grown, according to the government's 1996 Wiretap Report, to exceed 32% of all wiretaps conducted. Obviously, the wireless industry and law enforcement have a significant stake in a rapid, standardized implementation of CALEA.

Unfortunately, the FBI has not managed the implementation process well, and, despite the best efforts of industry, implementation of the CALEA is at a virtual stalemate. To wit:

- Although CALEA expressly prohibits law enforcement from requiring any specific design of systems or features or the adoption of any particular technology, law enforcement has rejected the industry standard, which is 100% compliant with CALEA, and instead promoted its own, alternative standard replete with exotic capabilities.
- Three years after enactment of CALEA, law enforcement still has not published a final notice of its capacity requirements.
- Although CALEA authorizes the Attorney General to pay telecommunications carriers for their reasonable costs of CALEA compliance, the FBI's proposed cost recovery rules would define an untold amount of existing equipment as not eligible for reimbursement.
- These delays by law enforcement make compliance with the October, 1998, final compliance date impossible for telecommunications carriers.

To break the CALEA stalemate, CTIA suggests that the following four inter-related issues be resolved concurrently:

- *Capability.* Law enforcement should drop its opposition to the adoption of industry standard SP-3580. The industry consensus standard provides 100% of the capabilities required by CALEA. The FBI wish list of enhanced services and features, assuming that each function is otherwise lawful, should be pursued outside of the standards process.
- *Capacity.* Law enforcement should publish a final capacity notice that reflects historical wiretap experience and reasonable future projections and acknowledge that the cost of capacity is to be borne by law enforcement.
- *Cost Reimbursement.* As the telecommunications industry has deployed thousands of switches or upgrades in that absence of a capability standard since CALEA was enacted, the January 1, 1995, grandfather date should be revised to reflect the date when standards are finalized.
- *Compliance Date.* The October 25, 1998, compliance date is not achievable. Reflecting the unanticipated delays in CALEA implementation, the compliance date should be revised to a date two years after the finalization of the CALEA capability standard.

CTIA has pledged its support of CALEA and is committed to breaking the current impasse. As an industry, we took seriously the admonitions of Congress to construe CALEA as both the floor and ceiling of electronic surveillance. We took seriously the obligation to protect the privacy of communications not authorized to be intercepted. And we took seriously, and continue to take seriously, our obligation to assist law enforcement in this endeavor. We look forward to the same sense of compromise and commitment from law enforcement beginning with their support for the immediate deployment of the proposed standard, extension of the compliance date, finalization of the capacity notice and revision of the January 1, 1995, grandfather date.

#### I. INTRODUCTION

The Cellular Telecommunications Industry Association ("CTIA") appreciates the opportunity to submit this testimony concerning the current state of implementation of the Communications Assistance for Law Enforcement Act ("CALEA") on this, the third anniversary of the Act. When CALEA was under discussion in the Congress in 1994, wireless communications providers served just 16 million customers. In three short years, the wireless industry has tripled and now serves over 50 million customers. CTIA represents providers of the commercial mobile radio services, including 48 of the 50 largest cellular providers, personal communications services, enhanced specialized mobile radio, and mobile satellite providers, and commercial mobile radio services equipment manufacturers.

In 1994, as president of CTIA, I joined FBI Director Freeh "with a gentleman's handshake" to support CALEA as a balanced bill that would ensure law enforcement's ability to conduct authorized wiretaps in the future without impeding the introduction of new technologies, features and services along the way. CALEA was the codification of the long-standing spirit of cooperation that has always existed between the telecommunications industry and law enforcement in the conduct of lawfully authorized surveillance.

Given that history of cooperation, it may be somewhat surprising to Congress that perhaps the best that can be said about the implementation of CALEA today is that the process has not been well managed by the FBI and we are not where we expected to be by this date. Nonetheless, I am proud to say that industry, led by the wireless community, has kept its part of the CALEA bargain by producing a standard for implementation of CALEA's capability requirements that is true to the letter and spirit of the law.

Industry's proposed standard—currently out for public comment and vote—meets *all* of the requirements of CALEA. Once implemented, criminals no longer will be able to use advance features such as call forwarding to evade lawfully authorized surveillance. Law enforcement will be able to identify the origin, destination and termination of all calls carried by a carrier to or from the target of surveillance. In short, the industry standard will bring law enforcement into the digital age, and keep them there, just as CALEA contemplated.

With this suite of surveillance capabilities poised for release, Congress may ask why there is any controversy over CALEA implementation today. The answer is that the FBI wants, and has demanded over the last three years, not a CALEA solution but rather an enhanced surveillance service replete with exotic capabilities that do not exist today and that would have extraordinary costs to develop—costs they expect to shift to the telecommunications industry under the rubric of CALEA.

In passing CALEA, Congress directed law enforcement to avoid "overbroad interpretation of the requirements" and sought to "ensure that there will be no 'gold-plating.'" But the temptation has been irresistible, particularly in regard to the development of the industry standard. Congress gave industry the "key role in developing the technical requirements and standards that will allow implementation of the requirements." But, law enforcement has attempted to substitute its own judgment for that of the standards-setting body.

For example, law enforcement has proposed its own competing standard—the Electronic Surveillance Interface ("ESI") document—which, not surprisingly, elevates electronic surveillance above ordinary call processing. The ESI contains such demands as interception and delivery of information within 500 milliseconds—several times faster than some current switching technologies actually react to dialed digits. The absence of such a capability, according to the FBI, renders the industry standard "deficient."

Industry has sought to curb these excesses in the course of producing its standard. At every seeming impasse, CTIA initiated efforts to resolve the matter, calling together legal summits when the scope and reach of CALEA legal terms such as "call-identifying information" were in dispute, seeking compromise when law enforcement demanded that mobile phones be used as tracking devices, and urging so-

lutions that would bring the standard to the street sooner. However, the FBI apparently prefers a club to consensus. They have repeatedly threatened to derail the standards process and to seek enforcement orders against carriers if all of its demands as reflected in the ESI are not met.

Due to the opposition of the FBI and its "all or nothing" strategy, the future of the standard now is in doubt. After the FBI's first attempt to block release of the industry standard earlier this year, the wireless industry asked the Federal Communications Commission ("FCC"), in its capacity as arbiter of disputes under CALEA, to adopt the standard and reject the gold-plating attempts of the FBI. Simultaneously, the standards body further refined the proposed standard in an attempt to accommodate more of law enforcement's concerns within the bounds of CALEA. Balloting on that standard will be complete in just another week and Congress will learn whether the FBI is serious about getting CALEA capabilities on the street as soon as possible.

The timely and cost-effective implementation of CALEA is of the utmost importance to CTIA's membership. Wireless wiretaps accounted for less than 25% of all wiretaps conducted in 1993. The wireless share of wiretaps has grown, according to the government's 1996 Wiretap Report, to exceed 34% of all federal wiretaps conducted. Obviously, the wireless industry and law enforcement have a significant stake in a rapid, standardized implementation of CALEA.

Yet, the FBI continues to hold the industry standard hostage. Moreover, the FBI has failed itself to fulfill its CALEA obligation to inform industry of anticipated surveillance needs in the coming years. Congress directed the Attorney General to complete this task within a year of CALEA's enactment. But just as with capability, law enforcement over-reached. The first attempt at producing a capacity notice was roundly criticized for its excess and the FBI was forced back to the drawing board. The FBI's second capacity notice equally was flawed. With only 306 state and federal wireless Title III wiretaps (not including trap and trace, and pen register) in 1996 across the entire nation and over the entire year, the FBI proposed in its second capacity notice to conduct as many as 20,100 actual wireless wiretaps of all types three years from now simultaneously; that is, on the same day. Not surprising, the FBI once again has gone back to the drawing board and industry awaits the next notice.

Against this backdrop, two dates loom large. First, industry has not stood still over the last three years. New services and equipment have reached the market since the CALEA "grandfather" date of January 1, 1995. Equipment, facilities and services installed or deployed after that date are required to be CALEA-compliant by October 25, 1998 or the carrier may face significant penalties. Law enforcement is required to pay to retrofit equipment in place before January 1, 1995.

Many of CTIA's members did not even exist when CALEA was passed, but now are faced with the costs of compliance when standards are not yet available. Congress expected that standards would be deployed quickly so that the impact of the transition to CALEA compliance would be minimal. That reality has not come to pass. Law enforcement cannot tell Congress with any certainty how much it will cost to retrofit grandfathered switches; and the delay in release of the standard makes it impossible for any carriers to meet the assistance requirements of CALEA by October 25, 1998 in a standardized way. Non-standard implementation of CALEA will ensure that the cost of compliance simply will spiral out of control. The two CALEA dates must be addressed comprehensively and soon.

The solution to CALEA implementation requires resolution of what I call the 4-C's: (1) immediate promulgation of the industry standard with only the *capabilities* required by CALEA; (2) final promulgation of reasonable *capacity* requirements as soon as practicable; (3) extension of the October 28, 1998 *compliance* date until standards are available; and (4) *cost* reimbursement for upgrades and retrofits, including those deployed after January 1, 1995, that depended on the availability of a standard to meet compliance.<sup>1</sup>

<sup>1</sup> Others appearing today will address the very serious privacy issues raised by law enforcement's surveillance demands. While not the focus of CTIA's testimony, we do not want to imply in any way that the privacy of our customers and other telecommunications users is not paramount. In drafting the industry standard, the wireless community in particular has been duly considerate of privacy concerns and the mandate of CALEA to protect the privacy of communications not authorized to be intercepted. The views of the Center for Democracy and Technology, for example, were considered in the standards process. CTIA believes that the proposed standard implements CALEA consistent with Title III of the Wiretap Act and the Electronic Communications Privacy Act.

## II. CAPABILITY AND THE COMPLIANCE DATE—TWO OF THE FOUR “C’S” THAT MUST BE ADDRESSED

Development of surveillance capability functionality and meeting CALEA's compliance date are inextricably intertwined. To appreciate the current state of CALEA implementation of capability and the prospect of meeting the October 25, 1998 compliance date, it is necessary to review the recent history of development of the capability standard.

It is important to understand that industry has exercised more than due diligence in the balanced implementation of CALEA's capability requirements. Balance is the key word because in passing CALEA, Congress sought to balance three important policies: “(1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies.” H. Rep. No. 103-827, 103d Cong., 2d Sess. (1994), *reprinted in* 1995 U.S.C.C.A.N. 3489, 3493 [“House Report”]. These purposes are of equal weight and must inform any understanding of the specific requirements of CALEA.

### A. *The Safe Harbor Standard to Meet CALEA's Capability Requirements*

Section 103 of CALEA imposes four specific requirements on telecommunications carriers: (1) isolate expeditiously the content of the targeted communications transmitted by the carrier within its service area; (2) isolate expeditiously information identifying the origin and destination of targeted communications, i.e., the numbers dialed to or from a target phone; (3) provide intercepted communications and call-identifying information to law enforcement so they can be transmitted over lines or facilities leased by law enforcement to a location away from the carrier's premises; and (4) carry out intercepts unobtrusively, so targets are not made aware of the interception, and in a manner that does not compromise the privacy and security of other communications. These assistance requirements were intended “to be both a floor and a ceiling” and Congress repeatedly “urge[d] against overbroad interpretations of the requirements.” House Report at 3490.

Congress gave industry the key role in developing the technical standards and requirements necessary to implement the assistance requirements of CALEA, stating:

The legislation provides that the telecommunications industry itself shall decide how to implement law enforcement's requirements. The bill allows industry associations and standard-setting bodies, in consultation with law enforcement, to establish publicly available specifications creating “safe harbors” for carriers. This means that those whose competitive future depends on innovation will have a key role in interpreting the legislated requirements and find ways to meet them without impeding the deployment of new services.

House Report at 3499.

Section 107(a) of CALEA creates a “safe harbor” for carriers who are “in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization” or by the FCC under Section 107(b), to meet the assistance capability requirements of Section 103. To obtain this “safe harbor,” in early Spring 1995—almost immediately after passage of CALEA—industry began to formulate a technical standard under the auspices of the Telecommunications Industry Association, an association accredited by the American National Standards Institute (“ANSI”) to set standards.

To put the process in perspective, on average, 40–50 representatives of carriers and manufacturers met for at least one week each month over the last two and one half years in different locations throughout North America to meld together a standard that could be implemented by dozens of manufacturers for several dozen current, and all future, platforms. In short, this was no mean task.

By October 1995, industry had produced a draft standard over 170 pages in length. The standard provided for such capabilities as intercepting call content when the target's facilities employed advanced calling features such as call forwarding as well as the identification of the numbers dialed by the target or to the target's phone, even when call forwarding features are utilized.

The standards meetings were open and law enforcement representatives attended each one, although they provided no significant technical contributions or assistance through Spring 1996—a full year after the meetings had commenced and months after the initial drafts of the standard had been created and the progression toward completion of the technical requirements commenced.

### *B. Hijacking the Standards Process*

In April 1996, the FBI began to circulate its Electronic Surveillance Interface ("ESI") document, which set forth its preferred delivery interface for intercepted communications and the features, capabilities and types of information that law enforcement believed carriers must deliver. The FBI touted this de facto standard as a "safe harbor" and encouraged manufacturers and carriers to adopt it even though CALEA expressly prohibits law enforcement from requiring any specific design of systems or features or the adoption of any particular technology to meet CALEA. 47 U.S.C. § 1003(b)(1). Of course, the ESI ignored the CALEA safe harbor requirement that any standard be publicly available because the ESI was distributed to carriers under a restrictive use legend.

Widespread industry criticism of the ESI made it clear that the ESI had no standing in the technical community and would not be accepted as the CALEA standard. The FBI then submitted the ESI to the industry standards group as a so-called "contribution" to the standards process. This tactic significantly disrupted and delayed the progress of the standard as industry engineers were required to reconcile the inconsistent ESI line by line with PN-3580, the industry document.

Nonetheless, the industry group took up the ESI and integrated many of its requirements into the industry draft standard. The industry approach was simple—if the requirement had a basis in CALEA and a clear legislative expression, it would be included in the standard. If there was not clear authority, the capability would be rejected. The standards group accommodated many of the functional requirements put forward in the ESI but several specific features were rejected.

For example, law enforcement demanded that industry provide electronic messages to indicate when, in the course of a conference call under lawful surveillance, a party joins or drops from the call. Law enforcement cites evidentiary needs for this capability—a capability that does not exist today—and asserts that such information is "call-identifying." Of course, when a party joins or drops from an existing call has nothing to do with the dialing or signaling information that routes a call through the network. Existing technical standards for wireless communications such as IS-41 do not accommodate the collection of such party add and drop information and no carrier today uses such information for billing purposes or otherwise. In short, while the capability certainly has investigative value for law enforcement, it is not covered by CALEA and therefore the standards group rejected the demand.<sup>2</sup>

After months of additional work, the standards body voted in early 1997 to issue PN-3580 as a full ANSI standard. This procedure allowed not only industry representatives to comment and vote on the standard, but also law enforcement agencies and non-traditional standards participants such as privacy advocates. Standards Proposal (SP)-3580 was issued for balloting in March 1997.

In response, the FBI produced over 70 pages of comments—most of which had been considered and rejected during prior standards meetings and most of which came from the ESI. The FBI advised law enforcement agencies around the nation that SP-3580 was a "disaster" for law enforcement and urged these agencies—none of whom actually participated in the standards meetings—to vote "no" on their ballot.

After the close of the ballot, the industry standards body met to consider all comments received. Despite further accommodations to law enforcement's views during these meetings, law enforcement repeatedly threatened to challenge the industry standard before the FCC as "deficient" if industry brought the standard out over law enforcement objections. The law enforcement "no" votes effectively stymied release of the proposed standard.

<sup>2</sup>The scope of the definition of call-identifying information has been the source of industry's greatest disagreement with law enforcement. The standards group took Congress at its word when it said call-identifying information "is typically the electronic pulses, audio tones, or signaling messages that identify the numbers dialed or otherwise transmitted for the purpose of routing calls through the telecommunications carrier's network. . . . 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." House Report at 3501. Conversely, the FBI has offered numerous interpretations of this definition from the broadest view so as to encompass any signal within a carrier's network—a concept they had to abandon for obvious reasons—to any signaling information perceptible to a call participant such as voice message waiting indicators or busy signals, to post cut-through signals such as bank account numbers or signals to customer premises equipment.

CTIA will not use this venue to review the legal issues raised by law enforcement's interpretation of call-identifying information. CTIA has asked the FCC to resolve whether the FBI's "punch list" of capabilities are required by CALEA. But, this is no reason to hold up deployment of the industry standard and the capabilities law enforcement and industry agree are required by CALEA.

### C. CTIA Petitions the FCC for Relief

Faced with the impasse due to law enforcement's actions, CTIA filed a petition with the FCC on July 16, 1997, under Section 107 of CALEA. A copy of that petition is attached as Attachment 1. CTIA's goal in doing so was to break the standards deadlock by asking the FCC to adopt the industry consensus document as the "safe harbor" standard under CALEA. As CTIA noted in its petition, the industry consensus document would provide 100% of the capabilities required by CALEA and would "ensure that a giant leap forward can take place in law enforcement's electronic surveillance capability in the near future." Because even at that date it would have been impossible to meet the October 25, 1998 CALEA compliance date, CTIA also asked the FCC to extend the compliance deadline until two years after adoption of the industry standard—a period of time recognized by both law enforcement and industry as necessary to build to and implement the standard.<sup>3</sup>

While the petition was pending but before the FCC took any action, the industry standards group met again. Given law enforcement's intractable position and the fact that there were significant changes to the proposed standard, the standards committee recommended that the proposed standard be distributed for another round of balloting. Accordingly, the proposed standard, as revised, was submitted for a second ballot with comments due by October 28, 1997. The industry group will meet on November 3, 1997 and again on November 19, 1997 to consider comments received by that date prior to deciding how to proceed.

Given the continued efforts by industry to resolve this impasse both within and outside the standards group, the FCC recently declined to act on the CTIA petition pending a report on the outcome of the pending balloting. See FCC Notice of Proposed Rulemaking, CC Docket No. 97-213, (Adopted: October 2, 1997; Released October 10, 1997). The FCC "encourage[d] the industry and law enforcement community to continue their efforts to develop the necessary requirements, protocols and standards." *Id.*, ¶44. Accordingly, the compliance clock continues to tick and neither industry nor law enforcement is closer to deployment of CALEA-compliant equipment, facilities or services. In no event is the October 25, 1998, compliance date feasible or practicable.

### III. CAPACITY—THE THIRD "C"—REMAINS A MYSTERY

Not only has industry been thwarted in its efforts to produce a safe harbor standard, but law enforcement has failed completely to promulgate the CALEA-mandated notice of actual and maximum capacity needed in the near term.<sup>4</sup> As Congress is well aware, the Attorney General's first attempt at estimating future capacity as some percentage of the installed network was an admitted failure resulting in the complete withdrawal of the first notice.

The second capacity notice<sup>5</sup> was equally flawed and subject to criticism.<sup>6</sup> First, like its predecessor, the notice anticipated a widespread expansion of wiretapping that simply could not be justified by reference to historical data. The historical data in the second capacity notice indicates that there were only 2,703 simultaneous wireless wiretaps at any one time during the period evaluated. For wireless alone, the FBI states that it needs the ability to conduct 12,000 simultaneous wiretaps (that is, on the same day) throughout the nation and that it may need as many as 20,100. This is an unprecedented expansion of capacity.

Moreover, the FBI has stated that each new switch or equipment deployed after publication of its final notice would be required to have full capacity; that is, the ability to conduct simultaneously the number of wiretaps specified for the service

<sup>3</sup>It should be noted that after CTIA filed its petition, certain privacy groups filed their own petition on August 11, 1997, urging the FCC to "institute a rulemaking proceeding to protect the privacy interests of the American public as the telecommunications industry and law enforcement proceed to implement CALEA, the digital telephony law." See Petition of the Center for Democracy and Technology and the Electronic Frontier Foundation at 1. The privacy interests specifically complained that the proposed standard went too far, especially in regard to providing location information on wireless intercepts that could be used to track individuals as well as the amount and nature of packet data provided on pen register and trap and trace orders.

<sup>4</sup>Section 104(a) of CALEA requires the Attorney General to publish *not later than one year after the date of CALEA's enactment* and after public notice and comment, a notice of the actual and maximum number of interceptions, pen registers and trap and trace devices law enforcement may simultaneously conduct by the date that is 4 years after enactment of CALEA. Then, within three years of that publication, carriers must ensure, subject to government reimbursement, that its systems can accommodate the actual capacity and expeditiously expand to the maximum capacity.

<sup>5</sup>62 Fed. Reg. 1902 (January 14, 1997).

<sup>6</sup>Rather than review in detail here the significant deficiencies of the second notice, CTIA attaches its comments to the FBI on the second notice as Attachment 2.

area in the notice. For example, the FBI states in its second capacity notice that its actual wiretap needs in New York are 181 actual wiretaps. Under the FBI's interpretation, each carrier in a given service area must meet the total capacity number. Whenever a carrier deploys a new switch after the date of the final capacity notice, it must meet the full number for that specific switch. In other words, the original capacity is replicated with each new switch deployed after the final notice. (Original capacity also replicates with each new entrant into the market, creating a latent surveillance capacity that is stunning in its breadth.) In essence, if this truly is the FBI's understanding of CALEA—and the FBI has said so publicly—law enforcement would obtain an ever-scaling surveillance capacity without public notice, comment or Congressional oversight and all at carrier expense.

What is more remarkable about the FBI's view of capacity is that the provision of more it occurs without carrier compensation. The FBI has stated publicly its view that, notwithstanding the express words of Congress, a carrier is responsible for providing capacity at no charge for any equipment, facilities or services deployed after the final capacity notice is published. To the contrary, Congress made it clear that "to the extent that industry must install additional capacity to meet law enforcement needs, [CALEA] requires the government to pay *all* capacity costs from the date of [CALEA's] enactment, including *all* capacity costs incurred after the four year transition period." House Report at 3497 (emphasis added). If government refuses to pay *all* capacity costs, carriers are deemed to be in compliance with the capacity notices issued under Section 104(e) of CALEA. Thus, CALEA provides carriers with a "safe harbor" for capacity by mandating that law enforcement pay for all capacity sought under Section 104 before carriers have any obligation to provide it. House Report at 3505.

Apparently, in the face of overwhelming criticism of its attempted expansion of wiretapping, the FBI has returned to the drawing board and no final notice has yet been promulgated. However, the FBI shows no sign of retreat from its unreasonable interpretation of the capacity requirements of CALEA.

As Congress should know, capacity and capability are intertwined. There can be no dispute that implementation of CALEA's *capability* requirements will be more efficient and cost-effective if *capacity* requirements are known. The FBI's delays in publishing a credible capacity notice has a direct impact on the cost to develop and deploy CALEA equipment and software. Congress expected the Attorney General to complete this task within a year of CALEA's enactment—we are now on the third anniversary of the act without an inkling of the government's capacity needs or any knowledge of when the information might be forthcoming.

CTIA urges Congress to exercise its oversight responsibility on this issue and to bring into alignment the capability and capacity compliance dates. This approach would bring rationality to a standards process that currently is designing capabilities without knowing "how much of them" are required.

#### IV. FULL CARRIER COST RECOVERY—THE FOURTH "C"

As illustrated in the capacity discussion above, the FBI has been engaged in a concerted effort to shift as many implementation costs to industry as possible, no doubt because of the limited funds available to compensate carriers for system upgrades. Nowhere is this effort more clear than in the cost recovery rules promulgated by the FBI.<sup>7</sup>

Section 109(e) of CALEA directs the Attorney General, after notice and comment, to establish regulations necessary to effectuate timely and cost-efficient payment to telecommunications carriers under CALEA. On May 10, 1996, the FBI initiated a rulemaking proceeding to implement the cost reimbursement provisions of CALEA.<sup>8</sup> The proposed rules were widely criticized for violating the statutory requirement that all reasonable costs incurred in upgrading and modifying equipment and facili-

<sup>7</sup> Section 109 of CALEA authorizes the Attorney General, subject to the availability of appropriations, to agree to pay telecommunications carriers for: (a) all reasonable costs directly associated with the modifications performed by carriers in connection with equipment, facilities, and services installed or deployed on or before January 1, 1995, to establish the capabilities necessary to comply with Section 103 of CALEA; (b) additional reasonable costs directly associated with making the assistance capability requirements found in Section 104 of CALEA reasonably achievable with respect to certain equipment, facilities, or services installed or deployed after January 1, 1995, in accordance with the procedures established in CALEA Section 109(b); and (c) reasonable costs directly associated with modifications of any of a carrier's systems or services, as identified in the Carrier Statement required by CALEA Section 104(d), which do not have the capacity to accommodate simultaneously the number of interceptions, pen registers, and trap and trace devices set forth in the Capacity Notice(s) published in accordance with CALEA Section 104.

<sup>8</sup> 61 Fed. Reg. 21936 (1995).

ties be reimbursed. CTIA comments on the proposed rule are attached as Attachment 3.

The FBI published its final rule implementing the cost reimbursement provisions of CALEA ("Final Rule") in the Federal Register on March 20, 1997, with an effective date of April 21, 1997.<sup>9</sup> The Final Rule, while clarifying some definitions, did not significantly alter the proposed rule with respect to the ability of wireless carriers to recover their costs.

For example, CALEA permits carriers to recover the costs of modifying telecommunications equipment and facilities "installed or deployed" on or before January 1, 1995.<sup>10</sup> The FBI defined "installed or deployed" to mean the same thing—essentially, plugged into the network and delivering service to customers—and in a way that makes an untold amount of existing equipment and facilities obsolete. To illustrate the point, assume that Carrier A has a particular switching platform installed or deployed on December 1, 1994—a month before CALEA's January 1, 1995, grandfather date. Carrier A, under CALEA and the Final Rule, would qualify for reimbursement to upgrade the switch for CALEA capabilities. But if Carrier B, on *that same date*, bought the identical switch, had it under contract for purchase or simply had it sitting in its warehouse waiting for use, according to the FBI, Carrier B would NOT qualify for reimbursement. The platform would not be installed or deployed; it would be obsolete.

Put another way, the FBI's Final Rule requires any switching platform integrated into a network after January 1, 1995, to be CALEA-compliant at the carrier's own expense even if that same switch type was commercially available prior to January 1, 1995, or installed elsewhere in the carrier's own network or in any other carrier's network.

The FBI also has initiated another rulemaking, requesting comments concerning when it is NOT obligated to pay carriers for upgrades to equipment or facilities that otherwise would qualify under the grandfather provisions discussed above.<sup>11</sup> Section 109(d) of CALEA provides that the installed or deployed network is deemed to be in compliance with CALEA *until the equipment, facility, or service is replaced or significantly upgraded or otherwise undergoes major modification*.<sup>12</sup>

Given its definition of installed or deployed, industry has every reason to expect that the FBI will use the opportunity to define these terms in a way that further shifts the burden of CALEA to carriers. For example, mere generic software upgrades that occur periodically in the wireless industry and that do not even affect surveillance capabilities could be grounds for shifting the costs of CALEA to carriers if the FBI determines the upgrade to be significant. Thus, a software upgrade to provide wireless enhanced 911 information, even though it has no effect on electronic surveillance, could result in a "significant upgrade," according to the FBI, thereby requiring a complete CALEA upgrade at the same time. The financial ramifications of this FBI CALEA theory cannot be overstated. CTIA comments on the proposed rulemaking are attached as Attachment 4.

While if successful, the FBI cost shifting strategy certainly would avoid some costs, it is not a strategy for funding necessary upgrades. The Omnibus Consolidated Appropriations Act for Fiscal Year 1997, Pub. L. 104-208, required the FBI to submit to Congress a CALEA implementation plan before funds could be expended from the newly-created Telecommunications Carrier Compliance Fund. The FBI submitted its plan in early Spring 1996; however, it made no disclosure regarding the costs to implement CALEA. The FBI plan merely proposed to spread the \$500 million appropriated when CALEA was passed over the following 5 years. CTIA joined others in criticizing this hollow approach by submitting to Congress a response to the FBI implementation plan. Remarkably, the FBI cannot state with any certainty today how much it will cost to upgrade per switch. Nor can they provide

<sup>9</sup> 62 Fed. Reg. 13307 (1997).

<sup>10</sup> 47 U.S.C. § 1008(e)(2)(A).

<sup>11</sup> See 61 Fed. Reg. 58,799 (Nov. 10, 1996).

<sup>12</sup> Section 109(d) specifically states:

(d) *Failure to Make Payment with Respect to Equipment, Facilities, and Services Deployed on or Before January 1, 1995*—If a carrier has requested payment in accordance with procedures promulgated pursuant to subsection (e), and the Attorney General has not agreed to pay the telecommunications carrier for all reasonable costs directly associated with modifications necessary to bring any equipment, facility, or service deployed on or before January 1, 1995, into compliance with the assistance capability requirements of section 103, such equipment, facility or service shall be considered to be in compliance with the assistance capability requirements of section 103 *until the equipment, facility, or service is replaced or significantly upgraded or otherwise undergoes major modification*.

any estimated costs for deploying the proposed industry standard plus the FBI punch list of additional enhanced services.

Apart from the offensive cost shifting aspect of the Final Rule, the FBI unnecessarily increases the costs of even seeking to recover actual and unavoidable expenses of retrofitting equipment. The FBI requires telecommunications carriers to enter into cooperative agreements with the FBI under the Federal Grant and Cooperative Agreement Act, 31 U.S.C. §6301 *et seq.*, in order to be reimbursed for the costs of upgrades and modifications. It is CTIA's belief that these agreements are inconsistent with CALEA, place unlawful limits on the recovery of carriers' costs, and subject carriers to contractual requirements not contemplated by CALEA—requiring for example, the transfer of certain data rights to the federal Government. The FBI's imposition of contractual terms that it says carriers must agree to as a prerequisite to receiving reimbursement is inconsistent with CALEA.

Far from mandating the execution of such "cooperative agreements," CALEA specifies a claims process whereby telecommunications carriers may simply submit claims for the reimbursement of costs incurred for CALEA compliance. That simple structure has been subverted by FBI regulations. Rather, the rules look more like what one would have expected to see in regard to the government procurement of a weapons systems, except that even in the defense procurement area, the government has made great strides to streamline the process—not reflected in the proposed cooperative agreements.

These FBI procurement-like rules (a) require elaborate cost submissions with various categories of data to support them, (b) grant the FBI rights to acquire data rights in carrier intellectual property, (c) permit the FBI to conduct intrusive audits of the books and records of carriers and their subcontractors long after the requisite modifications have been completed and paid for, and (d) require, at least in the case of wireless carriers, restructuring accounting systems to meet FBI demands. This is not the timely and efficient claims submission process specified in CALEA—a process intended to make carriers whole through compensation for the taking of their property for the public purpose of conducting lawfully authorized electronic surveillance.

The cost reimbursement morass must be solved before CALEA can ever be implemented as Congress intended.

#### V. MOVING PAST THE BLOCKADE—CTIA'S RECOMMENDATIONS

It should be apparent from the above comments that CALEA implementation is off the tracks. The FBI has not managed the process well and, despite industry's best efforts, implementation is at a virtual stalemate. The balance struck three years ago has been perverted. CALEA has become the largest unfunded mandate in history, but with an unaccountable FBI imposing the cost burden on carriers and their customers.

The 4-C's discussed above must be resolved if the promise of CALEA is to be fulfilled. First, the industry consensus standard for providing CALEA capabilities must be promulgated now so that manufacturers can be assured that resources dedicated to systems engineering and design work will not be wasted. Simply put, absent the long-term assurances of an acceptable standard, no carrier or manufacturer will dedicate the resources necessary today when the work may be for naught tomorrow. The industry consensus standard provides 100% of the capabilities required by CALEA. The FBI punch list of enhanced services and features, assuming that each function is otherwise lawful,<sup>13</sup> should be pursued outside of the standards process.

Second, the CALEA compliance date of October 25, 1998, must be moved out until at least two years after the promulgation of the standard. Without this extension, carriers will seek non-standard solutions to meet CALEA rather than risk enforcement penalties. Such an approach will raise the cost for law enforcement significantly as they will have to find ways to receive delivery of surveillance information in as many ways as there are carriers. Further, once non-standard solutions are in place, carriers are not likely to then move to implement the standard because meet-

<sup>13</sup>The FBI has demanded the capability be built into the standard to monitor the held portion of a conference call whether or not the target of surveillance is present on the call. Certain privacy groups have objected to the capability on constitutional and statutory grounds, claiming that the demand fails particularity requirements. CTIA simply notes that the proposed standard does not address the desired capability because the demand really is a capacity issue—law enforcement may monitor one or more lines so long as it provisions the necessary circuits. If, however, despite being aware of the target's services, law enforcement simply provisions a single channel, the standard requires that channel follow the direction of the target's call. That is, if the target places a conference call on hold to take a call waiting or to initiate another call, the standard provides that the wiretap follows the target to the call waiting or new origination.

ing compliance in a non-standard way today at a much increased cost eliminates all of the cost-savings benefits of standardization tomorrow. In sum, the compliance date looms not only as an enforcement threat to carriers, but as a milestone for standardization of surveillance capabilities.

Third, law enforcement must finalize its capacity notice and do so in a reasonable manner consistent with the intent of Congress. Once final actual and maximum capacity numbers are known, carriers can plan for capacity increases. Ideally, capacity and capability can be planned for and developed concurrently to take advantage of design and scale efficiencies. Finally, law enforcement must acknowledge its obligation to fund capacity no matter when it is deployed.

Finally, the cost of implementing CALEA grows larger with new entrants to the telecommunications industry each day and expansion of existing carriers' networks. Law enforcement must prioritize its needs, fund the necessary retrofits and do so in a way that maximizes the reach of each dollar. This does not mean that law enforcement may shift the cost of necessary upgrades to carriers. The industry has demonstrated that it intends to do its part to implement CALEA even though the cost of deploying the proposed standard is growing to be enormous. Further adding to the cost burden likely will lead to petitions to the FCC for a determination that implementation of CALEA is not reasonably achievable.<sup>14</sup>

CTIA has pledged its support of CALEA and is committed to breaking the impasse. As an industry, we took seriously the admonitions of Congress to construe CALEA as both the floor and ceiling of electronic surveillance. We took seriously the obligation to protect the privacy of communications not authorized to be intercepted. And we took seriously, and continue to take seriously, our obligation to assist law enforcement in this endeavor. We look forward to the same sense of compromise and commitment from law enforcement beginning with their support for the immediate deployment of the proposed standard, extension of the compliance date, finalization of the capacity notice, and compensation for the reasonable costs of upgraded systems.

#### ATTACHMENTS

1. CTIA Petition For Rulemaking Before the Federal Communications Commission in the Matter of Implementation of Section 103 CALEA. July 16, 1997.
2. CTIA Comments on the Second Notice of Capacity Requirements Per Section 104 of CALEA. March 14, 1997.
3. CTIA Comments on the FBI's proposed cost recovery rules for CALEA. July 9, 1996.
4. CTIA Comments on the definitions of "Significant Upgrade" and "Major Modification" as used in implementation of Section 109 of CALEA. December 19, 1996.

---

#### ATTACHMENT 1

BEFORE THE  
FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON, D.C. 20554

In the Matter of  
Implementation of Section 103 of the  
Communications Assistance for Law  
Enforcement Act

To: The Commission

---

<sup>14</sup>Section 107 of CALEA provides that equipment, facilities and services are deemed compliant with CALEA unless law enforcement pays to make the upgrades reasonably achievable.

## PETITION FOR RULEMAKING

Michael F. Altschul  
Vice President, General Counsel

Randall S. Coleman  
Vice President for  
Regulatory Policy and Law

CELLULAR TELECOMMUNICATIONS  
INDUSTRY ASSOCIATION  
1250 Connecticut Avenue, N.W.  
Suite 200  
Washington, D.C. 20036  
(202) 785-0081

Albert Gidari  
PERKINS COIE  
1201 Third Avenue  
40th Floor  
Seattle, Washington 98101  
Of Counsel  
July 16, 1997

## SUMMARY

The Cellular Telecommunications Industry Association ("CTIA") brings this petition for rulemaking on behalf of its members to establish an electronic surveillance technical standard to implement Section 103 of the Communications Assistance for Law Enforcement Act ("CALEA"), P. L. 103-414, (1994), 108 Stat. 4279, *codified at* 47 U.S.C. § 1001 *et seq.*

The Federal Communications Commission ("Commission") does not begin this rulemaking on a blank slate. CTIA attaches to this petition the current industry consensus document that meets 100% of the assistance capability requirements of sections 103 and 106 of CALEA. The industry consensus document was intended to become the publicly available technical standard contemplated by Section 107(b) of CALEA and a "safe harbor" for telecommunications carriers and manufacturers that implement its technical requirements. However, the standards process is deadlocked, due in large measure to unreasonable demands by law enforcement for more surveillance features than either CALEA or the wiretap laws allow.<sup>1</sup>

Law enforcement has threatened to challenge the industry consensus document before the Commission as "deficient" under Section 107(c) of CALEA if it is promulgated without the additional, exotic capabilities it demands. Thus, law enforcement would delay implementation of a standard that is 100% CALEA-compliant to extract 110% of what Congress authorized.

CALEA specifically provides that the Commission shall resolve disputes in the standards process and issue a final electronic surveillance standard. CTIA asks the Commission to do so here, and in an expedited manner, to allow telecommunications carriers and manufacturers to bring CALEA-compliant equipment, services and facilities as soon as possible to law enforcement's arsenal of investigative tools.

By filing this petition, CTIA hopes to break the impasse and deliver a uniform standard for electronic surveillance sooner than otherwise would be possible. The Commission must act promptly to establish the standard and to define the obligations of telecommunications carriers under Section 103 during the transition period to the new standard.<sup>2</sup> CTIA's petition and the industry consensus document ensure

<sup>1</sup> The Commission should be aware that almost immediately after the passage of CALEA, industry took the lead to develop technical requirements that would be promulgated as an American National Standards Institute ("ANSI") standard. The standards setting process was delayed significantly by law enforcement actions, ranging from the production of a competing "standard" known as the Electronic Surveillance Interface ("ESI") document—something expressly prohibited by CALEA—to recently stuffing the standard ballot box with "no" votes from law enforcement agencies across the country, which guaranteed that no ANSI standard could be promulgated in a timely manner, if at all.

<sup>2</sup> Given these circumstances, it is virtually impossible for telecommunications carriers or manufacturers to implement the capability assistance requirements of Section 103 by October 25, 1998, the effective date of CALEA. Thus, the Commission will need to establish a reasonable time to implement the standard established pursuant to this petition.

that a giant leap forward can take place in law enforcement's electronic surveillance capability in the near future.

BEFORE THE  
FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON, D.C. 20554

In the Matter of

Implementation of Section 103 of the  
Communications Assistance for Law  
Enforcement Act

To: The Commission

PETITION FOR RULEMAKING

The Cellular Telecommunications Industry Association ("CTIA"), pursuant to Section 1.401(a) of the Federal Communications Commission's ("Commission") Rules and Regulations, 47 C.F.R. § 1.401(a), and Section 107(b) of the Communications Assistance for Law Enforcement Act ("CALEA"), 47 U.S.C. § 1006(b) (1994),<sup>3</sup> hereby submits this petition for rulemaking to implement Section 103 of CALEA. CTIA is a nonprofit corporation organized under the laws of the District of Columbia and is the principal trade association of the wireless communications industry. Membership in the association encompasses all providers of commercial mobile radio services and includes 48 of the 50 largest cellular and personal communications services and others with an interest in the wireless communications industry.

CTIA requests that the Commission promulgate, by rule, the industry consensus document, attached hereto as Exhibit 1, as the technical standard for the assistance capability requirements of Section 103 of CALEA, 47 U.S.C. § 1004. Under Section 107(b) of CALEA, in the absence of an industry standard, the Commission has authority to establish, by rule, technical requirements or standards that—

- (1) meet the assistance capability requirements of Section 103 by cost-effective methods;
- (2) protect the privacy and security of communications not authorized to be intercepted;
- (3) minimize the cost of such compliance on residential ratepayers;
- (4) serve the policy of the United States to encourage the provision of new technologies and services to the public; and
- (5) 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.

47 U.S.C. § 1006(b).

There is no final industry standard to implement CALEA and none can be promulgated in sufficient time to allow manufacturers to develop, and carriers to implement, CALEA compliant equipment, facilities or services by October 25, 1998—the effective date of CALEA Section 103. Even if the standards process could be completed in a timely way, the FBI has made clear it will challenge the current industry consensus document. Accordingly, the Commission must act promptly to establish the standard and to define the obligations of telecommunications carriers under Section 103 during the transition period to the new standard.

As set forth more fully below, the attached industry consensus document meets the first four factors of Section 107(b). The Commission itself must act to meet the fifth factor and CTIA specifically requests that the Commission set a date two years after final publication of the standard as a reasonable time for manufacturers and carriers to transition to the new standard. During the transition period, carriers should be obligated to provide technical assistance for electronic surveillance in accordance with 18 U.S.C. § 2518(4).

Absent Commission action, carriers and manufacturers will take steps to meet their CALEA obligations in a non-uniform manner. Section 107(a)(3) of CALEA provides that the absence of a standard or technical requirements does not relieve a carrier from its obligations under Section 103. In other words, carriers will be sub-

<sup>3</sup>In addition, the Commission has broad general powers under Section 301(a) of CALEA, which provides that the Commission "shall prescribe such rules as are necessary to implement the requirements of [CALEA]." 47 U.S.C. § 229(a).

ject to enforcement actions after October 25, 1998, and \$10,000/day fines until they achieve compliance. The result will be to increase complexity and cost for both law enforcement and carriers who otherwise would prefer a common delivery interface for electronic surveillance information.

CTIA's petition and the industry consensus document ensure that electronic surveillance capabilities that meet CALEA requirements can be deployed in the very near future. Additional capabilities demanded by law enforcement, if found to be lawful and reasonably achievable under CALEA, may be the subject of future standard revisions, but need not and should not delay or hinder immediate implementation of the standard.

#### I. BACKGROUND

CALEA became law on October 25, 1994. P.L. 103-414, 108 Stat. 4279 (1994). It requires telecommunication carriers "to ensure that new technologies and services do not hinder law enforcement's access to the communications of a subscriber who is the subject of a court order authorizing electronic surveillance."<sup>4</sup> H.R. Rep. No. 103-827 (1994), *reprinted in* 1995 U.S.C.A.N. 3489, 3496 [hereinafter "House Report"]. Section 103 of CALEA sets forth the capability assistance requirements that carriers must meet by October 25, 1998. Under Section 103, a telecommunications carrier must ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of:

(1) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission to or from the subscriber's equipment, facility, or service, or at such later time as may be acceptable to the government;

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

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

(B) in a manner that allows it to be associated with the communication to which it pertains,

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

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

<sup>4</sup>In addition, Section 104 of CALEA required the Attorney General, not later than one year after the date of enactment of CALEA, to publish notice of its capacity requirements in the Federal Register. The Attorney General subsequently delegated this responsibility to the Federal Bureau of Investigations ("FBI"). Federal Bureau of Investigations—General Functions [AG Order No. 1951-95], 60 Fed. Reg. 11906 (1995) (to be codified at 28 C.F.R. pt. 0). Capacity refers to the actual and maximum number of simultaneous wiretaps law enforcement expects to conduct 4 years after the date of enactment of CALEA. The first capacity notice was so widely criticized for requiring capacity to conduct wiretaps on 1 out of every 100 calls that the FBI withdrew it and began anew. See Implementation of Section 104 of the Communications Assistance for Law Enforcement Act, 62 Fed. Reg. 1902, 1903-04, 1909 (Dept. Justice 1997). The second notice was equally flawed and beyond what CALEA required, calling for in excess of one hundred thousand wiretaps in some metropolitan areas. The FBI has yet to issue a final notice, so as of the date of this filing, the industry still does not know the amount of capacity it must design into its systems. Under Section 104(a), industry will not have to comply with the capacity requirements until 3 years after final promulgation of the notice, which means no earlier than the year 2000.

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

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

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

Congress intended the assistance requirements "to be both a floor and a ceiling." House Report at 3502. As FBI Director Freeh testified before Congress, the legislation was intended to preserve the status quo and provide law enforcement with no more and no less access to information than it had in the past. *Id.* Congress thus "urge[d] against overbroad interpretation of the requirements." *Id.*

Congress gave industry, in consultation with law enforcement, and subject to Commission review, the key role in developing the technical requirements and standards to implement Section 103 of CALEA. Section 107(a)(2) of CALEA specifically delegates to industry associations or standard setting organizations the right to establish standards for implementation of Section 103 capability assistance requirements. Congress stated:

The legislation provides that the telecommunications industry itself shall decide how to implement law enforcement's requirements. The bill allows industry associations and standard-setting bodies, in consultation with law enforcement, to establish publicly available specifications creating "safe harbors" for carriers. This means that those whose competitive future depends on innovation will have a key role in interpreting the legislated requirements and find ways to meet them without impeding the deployment of new services.

House Report at 3499.

In the absence of an industry standard, Congress empowered the Commission to establish a standard by rule. 47 U.S.C. § 1006(b). Here again, Congress specifically directed industry, law enforcement and the Commission "to narrowly interpret the requirements" of CALEA. House Report at 3503.

Section 107(a) of CALEA creates a "safe harbor" for carriers who are "in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization, or by the Commission under (Section 107(b)), to meet the [assistance capability] requirements of section 103." To obtain this "safe harbor," in early Spring 1995—almost immediately after passage of CALEA—industry began to formulate a technical standard under the auspices of the Telecommunications Industry Association ("TIA")<sup>5</sup> to implement Section 103. Project number (PN) 3580 was assigned to the standard work under TIA's Subcommittee TR45.2. Representatives of carriers and manufacturers have met monthly since then to develop the standard. Law enforcement representatives have attended and participated in each of the meetings.

By October 1995, the industry document was 170 pages long and the standards work was well on its way to completion. It was not until April 1996 that the FBI began to circulate its Electronic Surveillance Interface ("ESI") document, which purported to set forth its preferred delivery interface for intercepted communications and the features, capabilities and types of information that law enforcement believed carriers must deliver. The FBI characterized the ESI as "safe harbor"—creating a de facto standard—even though CALEA expressly prohibits law enforcement from requiring any specific design of systems or features or the adoption of any particular technology to meet CALEA. 47 U.S.C. § 1002(b)(1).

Widespread industry criticism of the ESI, which was not publicly available due to a restrictive use legend, made it clear that the ESI had no standing in the technical community and would not be implemented whole cloth as the CALEA standard. The FBI then submitted the ESI to the standards group as a "contribution" to the standards process, significantly disrupting and delaying technical standards development as industry engineers were required to reconcile line by line the inconsistent ESI with PN-3580.

Nonetheless, the industry group took up the ESI and integrated most of the requirements into the industry document. The industry approach was simple—if the requirement had a basis in CALEA and a clear legislative expression, it would be included in the standard. If there was not clear authority, the capability would be

<sup>5</sup>TIA is accredited by the ANSI. TIA sponsors engineering committees to develop standards. TIA's TR-45.2 subcommittee is the engineering committee designated to produce the lawfully authorized electronic surveillance standard under project number 3580.

rejected. In the end, the current industry consensus document meets 100% of CALEA's requirements.

TR45.2 voted to issue PN-3580 as an ANSI standard in order to seek the widest range of comment on the standard and its compliance with CALEA. This procedure would allow not only industry representatives to comment and vote on the standard, but also law enforcement agencies and nontraditional standards participants such as privacy advocates. Standards Proposal (SP)-3580 was issued in March 1997. TR45.2 had a closing date of May 12, 1997 whereas the ANSI ballot period extended to June 25, 1997.

In the TR45.2 voting, the FBI produced over 70 pages of comments seeking capabilities that had been considered and rejected during prior standards meetings and most of which came from the ESI. The FBI advised law enforcement agencies around the nation that SP-3580 was a "disaster" for law enforcement and urged them to vote "no" on their ballot. Local law enforcement agencies simply attached the FBI's 70 page critique of the proposed standard to their ballot responses. Of the 60 votes received, 34 "no" votes came from law-enforcement. The remainder predominantly supported the standard with technical comments. Receipt of ANSI ballots are still being calculated, but it appears that another 10 "no" votes were received from law enforcement. This ballot box stuffing has further delayed the standards process.

During the week of July 7th, the TR45.2 committee met to consider carefully each of law enforcement's over 165 comments on the proposed standard. Many more law enforcement recommendations were included in the industry consensus document, making CALEA requirements more clear to manufacturers and carriers. However, the disputed capabilities were not included, such as the ability to monitor the held portion of a conference call when the target is not on the line. No resolution was reached on the disputed features, which law enforcement characterized as "show stoppers" in terms of supporting any standard.

Thus, the TIA standards process will not yield a standard in sufficient time to permit industry-wide implementation by the October 1998 compliance deadline. The absence of a uniform standard will result in a patchwork of carrier-specific solutions as carriers expend time and resources to comply with the law and will greatly decrease the likelihood that a uniform standard will be developed and implemented by industry. Divergent solutions also will increase the overall costs of compliance to the detriment of carriers, their subscribers, and law enforcement which will be required to be able to accept delivery of intercepted communications in a variety of non-standard formats. In sum, the absence of a standard benefits no one.<sup>6</sup>

## II. DISCUSSION

Under Section 107(b) of CALEA, in the absence of an industry standard, the Commission has authority to establish, by rule, the technical requirements or standards to implement Section 103 of CALEA. Further, under Section 301(a) of CALEA, the Commission has broad authority to issue rules to implement CALEA generally. As noted above, there is no final industry standard and none can be promulgated in sufficient time to allow manufacturers to develop, and carriers to implement, CALEA compliant equipment, facilities or services by October 25, 1998—the effective date of CALEA Section 103. Accordingly, the Commission has jurisdiction to act upon CTIA's petition. In doing so, the Commission has five factors to consider, each of which is discussed below.

### *(1) The Industry Consensus Document Meets 100% of the Assistance Capability Requirements of Section 103 by Cost-Effective Methods*

The industry consensus document attached to this petition fully meets Section 103 requirements. The standard defines the interfaces between a telecommunications carrier and a law enforcement agency to assist the agency in conducting lawfully authorized electronic surveillance. As the industry consensus document explicitly states, its purpose is to facilitate compliance with the assistance capability require-

<sup>6</sup> TIA recently responded to a claim by the FBI to ANSI that the standards process was unfair by stating that the FBI had every reason to use such frivolous claims as a means to delay publication of a standard. TIA noted that the FBI would use its enforcement powers to extract concessions from carriers that, due to the absence of a standard, were not able to comply with CALEA by October 1998. Moreover, TIA noted, the FBI has a motive to delay implementation under a standard because as carriers upgrade embedded communications systems (those in service before January 1, 1995), the cost of compliance shifts from the government to the carriers. While FBI intransigence in industry meetings may lend support to TIA's view, CTIA believes that all parties will benefit immediately from the promulgation of a standard. The FBI has since withdrawn its appeal.

ments of Section 103 of CALEA. The document is based upon analyses of widely deployed communications services, ranging from plain old telephone service to integrated services digital network services.

Cost was not an element considered in the standards process. Rather, the TR45.2 committee considered only the requirements of CALEA and the technical means to implement them. However, CTIA believes that the industry consensus document represents the most cost-effective method of meeting Section 103 in the immediate future. Any other approach would require the Commission to seek comment and make findings on the record under Section 107(b) regarding the implementation cost of any alternative. Certainly, a non-standard approach to compliance must be avoided if costs are to be kept low.<sup>7</sup>

*(2) The Industry Consensus Document Protects the Privacy and Security of Communications Not Authorized to be Intercepted*

The industry consensus document meets this requirement by providing only that information authorized by CALEA to be delivered to law enforcement. The FBI has insisted throughout this process on additional capabilities that go beyond current wiretap functions and therefore implicate significant privacy concerns such as the demand to acquire network signaling information that notifies a subscriber that voice mail is waiting; wireless location information about a subscriber as he or she roams between cell sites, and multi-party calling information, including the identities of all parties to a conference call as they join or leave it, whether or not the subject is or ever was on the line.

Industry has rejected these demands and does not believe that a standard should be delayed pending resolution of these capability issues.

*(3) The Industry Consensus Document Minimizes the Cost of such Compliance on Residential Ratepayers*

CTIA believes this consideration would be satisfied if the industry consensus document becomes the standard because it will represent the most cost-effective implementation plan, which then results in the least impact to subscribers.

*(4) The Industry Consensus Document Ensures that the Policy of the United States to Encourage the Provision of New Technologies and Services to the Public is Served*

The industry consensus document allows for a broad array of implementation strategies, depending on the needs of the individual carrier. This flexibility, common in standards, is deemed ambiguous by law enforcement. They prefer a standard that is technically rigid, demanding for example, that all carriers use only X.25 protocols to deliver data to law enforcement despite the richness of delivery methods available today. The FBI proposal would lock in yesterday's technology.

To protect against excessive and costly burdens on the telecommunications industry which might impair technological development, CALEA established a reasonableness standard for compliance of carriers and manufacturers with its requirements. The "reasonableness" criteria is prevalent throughout the statute. For example, in addition to cost-effective implementation of Section 103 noted above, the commission is directed, in Section 109(b), to consider eleven factors in assessing whether compliance is "reasonably achievable."<sup>8</sup> These factors were designed to give the

<sup>7</sup>The Commission should be aware that Section 107(c) of CALEA provides that a telecommunications carrier may petition the Commission for one or more extensions of the deadline for compliance with the capability requirements of CALEA. 47 U.S.C. § 1006(c). The Commission may grant an extension if it determines that compliance is not reasonably achievable through application of technology available within the compliance period. 47 U.S.C. § 1006(c)(2). The absence of a standard *a fortiori* means that compliance is not "reasonably achievable" through application of technology available within the compliance period." Thus, if the Commission acts promptly on CTIA's request, it may avoid hundreds of extension requests under Section 107(c) in the very near future as carriers and manufacturers seek to protect themselves from enforcement actions that could otherwise be brought. Of course, Section 107(c) provides an alternative ground for the Commission to issue an omnibus rule that suspends CALEA compliance activities until an appropriate standard is in place. In any event, establishing the industry consensus document as the standard now will bring CALEA-compliant technology to the market much quicker than any other approach, which CTIA believes will make such technology more cost-effective.

<sup>8</sup>The Section 109(b) factors include: (1) the effect on public safety and national security; (2) the effect on rates for basic residential telephone service; (3) the need to protect the privacy and security of communications not authorized to be intercepted; (4) the need to achieve the capability assistance requirements of Section 103; (5) the effect on the nature and cost of the equipment, facility, or service at issue; (6) the effect on the operation of equipment, facility, or service at issue; (7) the policy of the United States to encourage the provision of new technologies and services to the public; (8) the financial resources of the telecommunications carrier; (9) the effect

Commission direction to realize several policy goals: (a) costs to consumers are kept low; (b) the legitimate needs of law enforcement are met while preventing the "gold-plating" of law enforcement's demands; (c) privacy interests are protected; and (d) the goal of encouraging competition in all forms of telecommunications is not undermined, ensuring that wiretap compliance is neither used as a sword or a shield.<sup>9</sup>

*(5) The Industry Consensus Document Provides a Reasonable Time and Conditions for Compliance with and the Transition to Any New Standard*

The industry stands ready to implement the attached industry consensus document within two years of the Commission establishing the standard. However, given the current circumstances, it is virtually impossible for telecommunications carriers or manufacturers to implement the capability assistance requirements of Section 103 by October 25, 1998, the effective date of CALEA.

It is widely understood that manufacturers need adequate time to develop and design the software that will meet any standard. Indeed, in its implementation plan submitted to Congress in March 1997, the FBI admitted that standard industry practice requires 6 months of system engineering followed by at least 12 months engineering development before system deployment can begin. Carriers also need sufficient time to modify any equipment, facilities or services and to test the implementation. Two years from the date the Commission establishes the standard is reasonable and reflects the spirit and intent of CALEA.

In the interim, the Commission must define the obligations of carriers during the transition period to the new standard. CTIA recommends that the commission adopt the current requirement from Section 2518(4) of title 18, U.S. Code, which provides that a carrier must furnish law enforcement with "all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services" of the subject. This would preserve the status quo and guarantee continued assistance to law enforcement through the transition period.

### III. CONCLUSION

For the above stated reasons, the Commission should commence a rulemaking to establish a uniform standard for compliance with the assistance capability requirements of CALEA and adopt the industry consensus document attached to this petition. Commission action now would ensure a timely implementation of valuable law enforcement investigative tools that maintain the status quo of the scope of electronic surveillance while keeping law enforcement current with technological developments that otherwise might impede electronic surveillance.

Respectfully Submitted,

MICHAEL F. ALTSCHUL, *Vice President  
and General Counsel.*

RANDALL S. COLEMAN, *Vice President,  
Regulatory Policy & Law.*

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

Of Counsel

July 16, 1997

---

on competition in the provision of telecommunications services; (10) the extent to which the design and development of the equipment, facility, or service was initiated before January 1, 1995; and (11) such other factors as the commission determines are appropriate.

<sup>9</sup> 140 Cong. Rec. 10771, 10781 (Oct. 4, 1994) (comments by Rep. Markey).

## ATTACHMENT 2

CELLULAR TELECOMMUNICATIONS  
INDUSTRY ASSOCIATION (CTIA),  
Washington, DC, March 14, 1997.

DAVID WORTHLEY, *Unit Chief,*  
*Federal Bureau of Investigation,*  
*Telecommunications Industry Liaison Unit,*  
*Chantilly, VA.*

Re: Comments on the Second Notice of Capacity Requirements Per Section 104 of the Communications Assistance for Law Enforcement Act ("CALEA")

DEAR MR. WORTHLEY: The Cellular Telecommunications Industry Association ("CTIA")<sup>1</sup> hereby submits its comments on the Second Notice of capacity requirements issued by the Federal Bureau of Investigation's ("FBI") Telecommunications Industry Liaison Unit ("TILU") to carry out the government's implementation responsibilities of the Communications Assistance for Law Enforcement Act of 1994 ("CALEA").<sup>2</sup> CTIA previously submitted comments pursuant to the original February 13, 1997 filing deadline. On that day, however, the FBI announced that it would extend its comment deadline to March 15, 1997. The comments submitted herein reflect developments that have occurred since the original February 13 deadline. Specifically, in light of conflicting statements that have been made regarding interpretation of the Second Capacity Notice, the FBI must clarify—on the record—whether the capacity requirements reflect requirements on a switch-by-switch basis. Additionally, the FBI must clarify other ambiguities in the Second Notice, including whether the stated capacity requirements reflect total "engineering" capacity (i.e., total number of circuits) and the extent to which new carriers will be reimbursed for capacity modifications. The FBI must also re-evaluate the historical, actual, and maximum number of simultaneous interceptions to reflect accurate calculations on a per-switch basis.

I. THE FBI MUST CLARIFY THAT THE CAPACITY REQUIREMENTS IN THE SECOND NOTICE REFLECT THE NUMBER OF REQUIRED INTERCEPTIONS PER SERVICE AREA

The FBI has made several conflicting statements about how the capacity requirements in the Second Notice should be interpreted. The FBI has stated at open industry meetings that the number of simultaneous interceptions stated in the Second Notice reflect interceptions that each switch within a specified service area must accommodate. After CTIA filed its initial comments on the Second Notice indicating that this statement had been made, the FBI then stated at a press conference that "We never planned to require the industry to meet capacity requirements on a switch-by-switch basis. That would be crazy."<sup>3</sup> The FBI should formally address this discrepancy in the record of this proceeding.

As discussed previously, an interpretation that would subject each switch per service area to the stated capacity requirements is fundamentally inconsistent with the basis used by the FBI to calculate the numbers themselves, and imposes an unnecessary and onerous burden on the industry. Such an interpretation also creates a major cost reimbursement issue for the government.<sup>4</sup> The FBI should clearly state on the record that the capacity requirements reflect the number of simultaneous interceptions required per service area and will be allocated among all carriers in the particular service area on a switch-by-switch basis.

<sup>1</sup> CTIA is the international organization of the wireless communications industry for both wireless carriers and manufacturers. Membership in the association covers all Commercial Mobile Radio Service ("CMRS") providers, including 48 of the 50 largest cellular, broadband personal communications services ("PCS"), enhanced specialized mobile radio, and mobile satellite services. CTIA represent more broadband PCS carriers and more cellular carriers than any other trade association.

<sup>2</sup> See Public Law 103-414.

<sup>3</sup> James Kallstrom, FBI, quoted in The New York Times, "Dispute Arises Over Proposal for Wiretaps," Feb. 14, 1997. In addition to the public statement made by Mr. Kallstrom, a subsequent letter from David Worthley, Chief of the Telecommunications Industry Liaison Unit of the FBI also indicated that the numbers in the Second Notice "reflect intercepts per service area and not by switch." See Letter to Ed Hall, CTIA, from David Worthley, FBI, Feb. 28, 1997. Given the fundamental nature of this issue, such statements should be included in the formal record of the proceeding and accessible by the general public.

<sup>4</sup> See CTIA Comments at Section 11 (Feb. 13, 1997).

II. OTHER AMBIGUITIES REGARDING INTERPRETATION OF THE SECOND NOTICE SHOULD BE CLARIFIED

In addition to clarifying the fundamental issue of how the numbers represented in the Second Notice should be interpreted, the FBI also must clarify other ambiguities in the Second Notice, including whether the stated capacity requirements reflect total "engineering" capacity (i.e., total number of circuits) and the extent to which new carriers will be reimbursed for capacity modifications. The FBI also must re-evaluate the historical, actual, and maximum number of simultaneous interceptions to reflect accurate calculations on a per-switch basis. These issues have been discussed in detail in CTIA's comments of February 13, 1997.

III. CONCLUSION

For the reasons stated above, CTIA requests that the FBI formally clarify that its capacity requirements do not reflect requirements on a per switch basis but, rather, represent requirements for the entire service area. CTIA also requests that the requirements be adjusted to reflect actual engineering capacity in terms of circuits per switch, that the capacity reimbursement provisions allow reimbursement for new entrants as well as incumbent carriers, and that the estimated number of interceptions be reevaluated to create consistent requirements across all wireless services.

Sincerely,

WENDY C. CHOW, *Staff Counsel.*

ATTACHMENT 3

CELLULAR TELECOMMUNICATIONS  
INDUSTRY ASSOCIATION (CTIA),  
*Washington, DC, July 9, 1996.*

Mr. WALTER V. MESLAR, *Unit Chief,*  
*Telecommunications Contracts and Audit Unit,*  
*Federal Bureau of Investigation,*  
*Chantilly, VA.*

*CTIA Comments on Proposed Cost Recovery Rules*

DEAR MR. MESLAR: The Cellular Telecommunications Industry Association<sup>1</sup> ("CTIA") hereby submits its comments on the procedures proposed by the Federal Bureau of Investigation ("FBI") whereby telecommunications carriers can recover the costs associated with complying with the Communications Assistance for Law Enforcement Act of 1994 ("CALEA").<sup>2</sup> As you know, CALEA requires telecommunications carriers to ensure law enforcement's ability, pursuant to court order or other lawful authorization, to intercept communications notwithstanding advanced telecommunications technologies.

I. CAPABILITY AND CAPACITY REQUIREMENTS MUST FIRST BE DEFINED

First and foremost, it is not reasonable to require carriers to provide meaningful comments on the cost recovery rules proposed to implement Section 109 of CALEA in the absence of the specific capability and capacity requirements required by Sections 103 and 104 of CALEA.<sup>3</sup>

On January 16, 1996, CTIA and other interested persons filed comments on the FBI's Notice of Initial Capacity Requirements.<sup>4</sup> Today, nearly six months later, the FBI has not responded to these comments.<sup>5</sup> CTIA has a number of concerns regard-

<sup>1</sup>CTIA is the international trade association of the wireless communications industry. Membership in the association covers all Commercial Mobile Radio Service providers, including cellular, PCS, Enhanced Specialized Mobile Radio, and mobile satellite services, as well as others with an interest in the wireless industry.

<sup>2</sup>Public Law 103-414; 47 U.S.C. 1001-1010.

<sup>3</sup>Section 103 of CALEA describes the Assistance Capability Requirements that a telecommunications carrier must provide to federal, state, and local law enforcement agencies to conduct court-authorized electronic surveillance. Section 104 of CALEA requires law enforcement to notify telecommunications carriers, manufacturers, and support services providers of the actual and maximum number of communications intercepts, pen registers, and trap and trace devices that law enforcement agencies may conduct and use simultaneously.

<sup>4</sup>The proposal was published in the *Federal Register* on October 16, 1995. See 60 *Federal Register* at 53643.

<sup>5</sup>At a recent industry standards meeting, the FBI advised industry participants that it is still reviewing the procedures for calculating capacity requirements and will not publish their revised

ing both the capacity and capability requirements being proposed by the FBI, since these requirements will determine the costs that are subject to the Section 109 reimbursement procedures.<sup>6</sup>

At present, the wireless industry is not able to calculate the necessary port capacity required to meet law enforcement's needs. Without such knowledge, carriers cannot estimate the magnitude of their CALEA compliance costs, and without knowing the magnitude of their CALEA compliance costs, carriers cannot evaluate how the proposed cost allocation rules (both for pre-CALEA cost allocations, and for the proposed cost estimate submissions) apply to their systems.

Moreover, a new and entirely separate set of concerns and uncertainties has been raised over the capabilities that wireless carriers must provide law enforcement pursuant to CALEA. At the June 26, 1996, meeting of the TR 45.2 subcommittee at TILU Headquarters, the capabilities carriers must provide to law enforcement were set forth in the FBI's Electronic Surveillance Interface ("ESI") document. The ESI document seeks to provide carriers with the requirements of a compliance "safe harbor" for meeting CALEA's capability assistance requirements. Based on the FBI's description of these "safe harbor" requirements, the wireless industry believes that the ESI document requires far more equipment and functionality than is required by CALEA's statutory requirements.<sup>7</sup>

In what appears to be a classic bureaucratic SNAFU, the ESI document was prepared by the FBI's Telecommunications Industry Liaison Unit ("TILU"), with no apparent coordination with the FBI's Telecommunications Contracts and Audit Unit ("TACU"), the organization responsible for the proposed cost reimbursement rules. Thus, at last month's TR 45.2 subcommittee meeting, TILU presented its set of capabilities requirements for a compliance "safe harbor"—which CTIA believes extend well beyond the CALEA statutory requirements—while TACU advised participants that it will independently determine whether a carrier's deployment or modification of equipment, facilities, or services was required by CALEA and therefore whether the associated costs are eligible for reimbursement. Thus, carriers are confronted with a classic "Catch 22": they can comply with the TILU ESI "safe harbor" document and still risk having TACU determine that costs associated with such compliance are not mandated by CALEA. In other words, the costs required by TILU could be deemed not eligible for reimbursement by TACU. CTIA believes that the proposed rules must be revised to expressly state that carriers' costs associated with meeting the "safe harbor" standard meet the threshold determination that they are CALEA-mandated, and thus eligible for reimbursement.<sup>8</sup>

## II. WIRELESS CARRIERS REQUIRE DIFFERENT RULES

Throughout the proposed rules, there are assumptions that may apply to Local Exchange Carriers ("LECs") but that definitely do not apply to CMRS carriers. For example, Section 100.12 defines a cost as "reasonable" if, "in its nature and amount, it does not exceed that which would be incurred by a prudent person in the conduct of *competitive business*." (emphasis added). CMRS carriers are competitive businesses. There are two cellular carriers in every market, three broadband PCS licenses, and three additional broadband PCS licenses to be awarded, plus Specialized Mobile Radio and Enhanced Specialized Mobile Radio carriers.<sup>9</sup> Thus, are all CMRS carriers' costs presumed reasonable, despite the contrary presumption set forth in Section 100.12(a)(2)?

Similarly, Section 100.19(c) provides that if the FBI determines that a cost reduction should be made, carriers are prohibited from raising as a defense that the subcontractor "was a sole source supplier or otherwise was in a superior bargaining po-

---

capacity requirements prior to the third quarter of 1996. Telecommunications Industry Association Committee TR 45.2 Ad Hoc for Lawfully Authorized Electronic Surveillance, June 26-27, 1996, meeting at Telecommunications Industry Liaison Unit Headquarters, Chantilly, Virginia.

<sup>6</sup> As CTIA and other wireless commenters explained in their January 16, 1996, comments, the number of simultaneous voice channels is the relevant measure of a wireless system's capacity, not the percentage of "engineered capacity" proposed by the FBI. In addition, the FBI must clearly define the relevant service area for Category I, II, and III capacity requirements by county designation to reflect the breadth of wireless carriers' service areas.

<sup>7</sup> The specific capability concerns raised by the ESI Document go beyond the scope of these comments on the CALEA cost reimbursement rules. CTIA's will raise its concerns about the scope of the ESI Document separately.

<sup>8</sup> Similarly, TILU should state in its ESI document that TACU will recognize costs associated with a carrier's compliance with the "safe harbor" capabilities as being eligible for compensation under CALEA.

<sup>9</sup> For this reason, the FBI's Initial Regulatory Flexibility Analysis required by section 603 of the Regulatory Flexibility Act is flawed: CMRS carriers are not "dominant" within their markets, so they are not exempted from the category of "small" entities for the purposes of the Act.

sition and thus the costs of the agreement would not have been modified. . . .” In fact, wireless carriers will be forced to use sole source suppliers for nearly all of the necessary capacity and capability upgrades required by CALEA. This is because wireless carriers’ switches and radios do not have “open” architecture and interfaces, so only the switch vendor, as the sole source supplier, will be able to provide the needed upgrades and enhancements.<sup>10</sup>

Another flaw in the proposed rules is the FBI’s proposal of cost allocation rules that are more appropriate to the relatively static LEC environment, and that don’t conform to the realities of the wireless industry. The wireless industry is growing at approximately 40% a year, and carriers constantly are upgrading and expanding their network facilities to accommodate this growth.

January 1, 1995, is the cut-off date for determining which modifications are reimbursable under CALEA. Section 109(d) of CALEA requires that all equipment deployed before that date must be in compliance “unless such equipment, facility or service has been replaced or significantly upgraded or otherwise undergoes major modification.” The proposed rules do not provide sufficient guidance on pre-CALEA cost allocations to CMRS carriers who constantly are upgrading and modifying their networks. It is safe to say that most wireless carriers’ facilities are a combination of both pre-January 1, 1995, and post-January 1, 1995, assets. Section 100.13(a)(1) can be interpreted as barring wireless carriers from seeking recovery of costs which they incurred prior to January 1, 1995, and that otherwise would be recoverable under CALEA. Therefore, specific rules are required to identify allowable costs that are eligible for reimbursement under section 109(e) of CALEA.

CTIA previously raised another problem associated with the January 1, 1995, cut-off date. Broadband PCS licensees had not built their networks or begun service on January 1, 1995, and no funding has been proposed for reimbursement of their expenses to comply with the CALEA requirements. As of today, a number of PCS systems are operational and carriers are providing service to the public, while most of the other PCS licensees have designed and entered into procurement contracts for their networks and are installing their equipment while the FBI continues to deliberate on the CALEA capacity and capability requirements.

PCS carriers will have the same need to upgrade and modify their network facilities, equipment and services as cellular carriers. To preserve the regulatory parity afforded all CMRS carriers by FCC rule, the FBI cost recovery rules must be competitively neutral. Therefore, new rules must be proposed that reflect the need of all wireless carriers to engineer and procure upgrades and modifications to their networks and capabilities based on the FBI’s final determination of the CALEA requirements, and not on an arbitrary date whose application to determining carriers’ cost recovery eligibility would be capricious.

### III. PROPOSED RULES MUST BE REVISED

In addition to the more general comments raised above, CTIA urges the FBI to revise the following specific proposed rules.

*Section 100.15* defines allowable costs too narrowly. Congress intended to “pay all reasonable costs incurred by the industry” to comply with CALEA. H.R.Rep. No. 103-827, 103rd Cong., 2d Sess. 16 (1994). The FBI’s proposal to limit carriers’ cost recovery to only “direct costs” therefore is flawed. General and Administrative costs also should be allowable, as they are as real (and unavoidable) as an invoice from a vendor.

*Section 100.16* requires carriers to submit cost estimates. This requirement is unnecessary and burdensome. Carriers are required to submit actual cost data, based on their books of accounts. Therefore, not only is this requirement duplicative, it imposes a new and unwarranted compliance burden on carriers. Moreover, the detail specified in the proposed rule may not be available to the carrier, since the vendor may not have provided the carrier with level of detail proposed in this section.<sup>11</sup> CTIA urges the FBI to delete this provision.

<sup>10</sup> Another problem is raised by Section 100.19(c)(3) which holds carriers defenseless for their vendors’ failure to submit accurate cost data. Rather than base these rules on how the FBI expects carriers to maintain their books of account, it would be less burdensome (and more accurate) to base the rules on how vendors estimate and bill for equipment and feature upgrades.

<sup>11</sup> Given the way features and capabilities are “bundled” by vendors into a single software or equipment upgrade, even the manufacturer may not have sufficient cost detail.

## CONCLUSION

For all of the reasons stated above, the rules proposed to implement Section 109 of CALEA should be revised to accommodate the requirements of CMRS service providers.

Sincerely,

MICHAEL ALTSCHUL, *Vice President,  
General Counsel.*

## ATTACHMENT 4

CELLULAR TELECOMMUNICATIONS  
INDUSTRY ASSOCIATION (CTIA),  
*Washington, DC, December 19, 1996.*

TELECOMMUNICATIONS CONTRACTS AND AUDIT UNIT,  
*Federal Bureau of Investigation,  
Chantilly, VA  
Attn: CALEA FR Representative.*

Re: Comments Of The Cellular Telecommunications Industry Association On The Definitions Of "Significant Upgrade" And "Major Modification" As Used In Implementation Of Section 109 Of The Communications Assistance For Law Enforcement Act Of 1994.

TO WHOM IT MAY CONCERN: The Cellular Telecommunications Industry Association<sup>1</sup> (CTIA) is pleased to comment on the Federal Bureau of Investigation (FBI) request for suggestions on the definitions of "significant upgrade" and "major modification" as used in the implementation of the Communications Assistance for Law Enforcement Act of 1994<sup>2</sup> (CALEA). CTIA recognizes, however, that final arbitration of the use of these terms under CALEA will rest with the Federal Communications Commission or the Courts.

## I. LEGISLATIVE HISTORY

CALEA addresses "significant upgrade" in two places. First, with respect to enforcement orders, the Act states:

"an order enforcing the title may not . . . require a telecommunications carrier to modify, for the purpose of complying with the assistance capability requirements of section 103, any equipment, facility, or service deployed on or before January 1, 1995, unless the Attorney General has agreed to pay . . . for all reasonable costs directly associated with modifications necessary to bring the equipment, facility, or service into compliance with those requirements; or the equipment, facility or service has been replaced or significantly upgraded or otherwise undergoes major modification. (47 USC 1007 (c)(3)(B))

CALEA makes a second reference to significant upgrades in section 109, which referred to the failure of the government to make payments to carriers, and states that if a carrier has requested payment and;

"the Attorney General has not agreed to pay the telecommunications carrier for all reasonable costs directly associated with modification necessary to bring an equipment, facility, or service deployed on or before January 1, 1995, into compliance with the assistance capability requirements of section 103, such equipment, facility, or service shall be considered to be in compliance with the assistance capability requirements of section 103 until the equipment, facility, or service is replaced or significantly upgraded or otherwise undergoes major modification." (47 USC 1008 (d))

In the case of equipment deployed after January 1, 1995, CALEA states:

"if compliance with the assistance capability provisions of section 103 is not reasonably achievable . . . the Attorney General . . . may agree, subject to the

<sup>1</sup> CTIA is the international organization which represents all elements of the Commercial Mobile Radio Service (CMRS) industry, including cellular, personal communications services, enhanced specialized mobile radio, wireless data, and mobile satellite services. CTIA has over 750 total members including domestic and international carriers, resellers, and manufacturers of wireless telecommunications equipment. CTIA's members provide services in all 734 cellular markets in the United States and personal communications services in all 50 major trading areas, which together cover 95% of the U.S. population.

<sup>2</sup> Public Law 103-44; 47 U.S.C. 1001-1010.

availability of appropriations, to pay the telecommunications carrier for the additional reasonable costs of making compliance with such assistance reasonable achievable; and if the Attorney General does not agree to pay such costs, the telecommunications carrier shall be deemed to be in compliance with such capability requirements." (47 USC 1008 (b)(2)(A) and (B).)

These provisions make it clear that government must reimburse carriers for all but fundamental changes to equipment, facilities, or services deployed on or before January 1, 1995. In addition, even if major modifications are completed on such equipment, facilities, or services deployed after January 1, 1995, but before CALEA-compliant equipment is available, and, that modified equipment must be retrofitted once CALEA-compliant technology is available, then the cost of such retrofits should be reimbursed by the government as well. This payment by the government is necessary because compliance with CALEA cannot be considered "reasonably achievable" if CALEA-compliant technology is not commercially available. The framers of CALEA explain the government's responsibility to pay forcefully in the Act's legislative history:

Under, th[e] compromise, the near term costs for the next four years would *unequivocally* be borne by the government. Existing switches would be retrofitted with the software necessary to assure wiretap capability. Under this provision, absent a commitment by law enforcement to *pay fully* for the modifications, a carrier would be deemed in compliance with the law and no further action on its part would be required. [Emphasis added]

A second important provision will require that as new switching equipment and services are *designed and manufactured*, wiretapping capabilities [will] be assured. It is obviously much more economical to design the wiretapping access into the new equipment and services rather than to engage [in] after-the-fact and expensive retrofits. That requirement will, therefore, be part of the law. H. Rep. No. 103-827, 103rd Cong, 2d Sess., *reprinted in* 1994 U.S.C.C.A.N. 3489, 3515 (Additional views of Representatives Edwards and Boucher) [Emphasis added]

The black letter language of CALEA, as well as the Congressional intent as expressed by the additional views of the framers as reprinted above, make it absolutely clear that carriers should be reimbursed for the CALEA compliance costs for any equipment that was in use by any carrier prior to January 1, 1995, regardless of whether or not a specific carrier actually had a specific unit of grandfathered equipment in use before January 1, 1995. In other words, if the government is making CALEA compliance reimbursement payments to one carrier for a specific unit of grandfathered equipment, the government should make such reimbursements to all carriers who are also using that equipment. Whether or not a specific carrier had that unit of grandfathered equipment in use prior to January 1, 1995 is not relevant. For the government to pick and choose which carriers using grandfathered equipment should be made whole for CALEA compliance costs is to circumvent the Congress's mandate that the government "fully pay" the carriers' costs of compliance.

## II. DEFINITION OF SIGNIFICANT UPGRADE AND MAJOR MODIFICATION:

Given the intent of Congress to "fully pay" carriers' costs of CALEA compliance, CTIA believes that the following definitions will help guide the process of reimbursement:

*Deployed.* Equipment, facilities, or services are considered deployed under CALEA if they were commercially available to any carrier in the telecommunications industry on or before January 1, 1995. The carrier requesting payment is not required to have that unit of equipment in use as of January 1, 1995. In other words, if equipment, facilities, or services were deployed by one carrier prior to January 1, 1995, then those units of equipment, facilities, or services should be considered to be deployed by all carriers. This interpretation is vital in order to maintain competitive neutrality in the FBI's reimbursement rules.

*Replaced.* Equipment, facilities, or services are considered replaced under CALEA if they were commercially available to any carrier in the telecommunications industry before January 1, 1995 and are not an upgrade or modification of previously deployed equipment, facilities, or services.

*Significant Upgrade or Major Modification.* Equipment, facilities, or services are "significantly upgraded or otherwise undergo major modification within the meaning of CALEA if the core functionality of deployed equipment, facilities, or services is changed or altered significantly so as to provide new features or capabilities that, without meeting the assistance requirements of CALEA, would impede law enforce-

ment's ability to intercept all communications or access reasonably available call-identifying information.

### III. AN OPEN AND ACCOUNTABLE PROCESS FOR CARRIER REIMBURSEMENT IS NEEDED.

On May 10, 1996, the FBI published a proposed CALEA cost reimbursement rule (61 FR 21, 396) that proposed reimbursement procedures for CALEA compliance costs. In its response, CTIA on July 9th commented that the FBI's proposed rules did not take into account the dynamic and competitive nature of the wireless telecommunications industry and the associated rapid changes and improvements in equipment used to provide wireless services. The FBI has not yet addressed the concerns raised in CTIA's July 9th filing. Obviously, without flexible reimbursement rules and definitions of "significant upgrade" and "major modification" that are consistent with those offered above, the FBI could, as a method of cost containment, classify all post-January 1, 1995, modifications as replacements, major modifications, or significant upgrades. Such action by the FBI would defy the requirements of CALEA and the intent of Congress that the government "fully pay" carriers for the CALEA compliance costs. Accordingly, CTIA believes that the FBI should have in place open and accountable procedures to determine CALEA compliance costs and the associated carrier reimbursements, and that it is inappropriate for the FBI to negotiate private deals or "cooperative agreements" with individual carriers for what potentially may be large expenditures of public dollars. As with other government programs, citizens have a right to know how their tax dollars are being spent, and the FBI CALEA costs reimbursement process should provide the same level of accountability *during and after* the reimbursement process as other government programs.

CTIA also takes exception to the FBI's decision to separate the cost recovery reimbursement rulemaking from the definitional issues addressed in this filing. It is simply not practical to separate consideration of the operative definitions from consideration of the procedures used to compensate carriers. Just as the FBI's cost-recovery procedures should be open and accountable, the definitions used to determine the eligibility of equipment for compensation should be well defined, widely disseminated, and should consistently adhere to the FBI's regulations developed after standard notice and comment procedures.

### IV. CONCLUSION

The FBI should adopt the definitions of significant upgrade and major modification as presented in this filing and re-integrate consideration of these definitional issues back into its rulemaking on cost recovery. The cost recovery process, as well as the definitions used in that process to determine the eligibility of equipment for cost reimbursement, should be an open and accountable process that is established through proper notice and comment. Our Nation's taxpayers deserve no less. Finally, the grandfather date of January 1, 1995 should be changed to coincide with the government's release of its capacity requirements.

Sincerely,

JONAS NEIHARDT,  
*Director for Congressional Affairs.*

Mr. McCOLLUM. Thank you, Mr. Wheeler.  
Mr. Kitchen?

### STATEMENT OF JAY KITCHEN, PRESIDENT, PERSONAL COMMUNICATIONS INDUSTRY ASSOCIATION

Mr. KITCHEN. Thank you, Mr. Chairman, and members of subcommittee. It's my pleasure to be here with you today to talk about CALEA. As president of the Personal Communications Industry Association, I come before you with a slightly different perspective than some of the others testifying today. I represent the new entrants in the wireless communications industry, the personal communications services that Mr. Wheeler has talked about already.

I'm certain you know that these carriers have really revolutionized the wireless industry. Unfortunately, when it comes to CALEA, PCS carriers are facing challenges that we believe Congress never intended and, Mr. Chairman, I believe you, in your

opening remarks, and Mr. Meehan in his opening remarks, really framed the issue very well as to what we're facing here.

From the beginning, we've reached out to the FBI and the Department of Justice because we really want to help law enforcement to do its job. And I think our industry is very sincere about that. And to their credit, law enforcement officials have worked with us to establish a dialogue that was necessary to move this process forward, but we just haven't gotten all the way yet.

That dialogue has taken place over the course of the last year and has led us to believe that PCS compliance cannot happen unless Congress acts quickly to make some modest changes to CALEA. And while the testimony I submitted before you goes into greater detail regarding our difficulties in complying with the law, let me briefly outline some of those areas here this morning.

In order for PCS carriers to meet the requirements of CALEA, we need to have a compliant equipment that meets industry-adopted standards. But that equipment just doesn't exist today. Why? Because we have no technical standards. They just haven't been set. And what the industry is being asked to do is build a house without blueprints. And the standards are the blueprints that we need to shape the way the technology will work.

Let me be clear that until those standards have been set by law enforcement and industry and equipment and software have been produced by manufacturers and provided to carriers, we simply don't have the means to comply with the law. We just can't do it.

What makes that all the more disturbing, Mr. Chairman, is that under CALEA it's the carriers, many of which are small, start-up businesses in PCS that are struggling to survive, face penalties of \$10,000 a day for each and every day that compliance is not reached. And that is just grossly unfair.

Even more troubling is the fact that under CALEA, PCS carriers, unlike, perhaps, cellular and wireless carriers, cannot be reimbursed for the cost of upgrading their system. Systems that were deployed prior to January 1st of 1995 are either reimbursed for retrofitting or are automatically deemed in compliance. There's simply no justification to differentiate between PCS carriers, who came into existence after CALEA was written, and cellular and wire line. All of us have been prevented from complying with CALEA because of a lack of compliant equipment that meets this industry standard. It's only fair that all carriers either be eligible for reimbursement for retrofitting or be deemed in compliance.

If the law is not changed, PCS carriers will have to recover those costs somewhere, and the question needs to be asked, if not from Washington, who's going to pay for this mandate? Where will it come? From your constituents? Mr. Chairman, the nation's PCS carriers are being treated like second-class citizens who are being discriminated against. That's wrong, and we implore you to rectify this injustice.

I'd like to take the rest of my time to propose that Congress pass a fair and reasonable change to CALEA that would allow the wireless industry to make good on our unwavering commitment to help law enforcement do its job. We're serious about that.

Specifically, CALEA should be changed in the following manner. We need changes on the reimbursement and compliance date of at

least 18 or 24 months after standards are approved, and any equipment deployed prior to that time should be deemed in compliance. We also need changes that would allow the FBI to use the 500 million dollars already authorized to pay switch manufacturers directly for software upgrades that will make both pre-1995 and post-1995 switches CALEA-compliant.

Mr. Chairman, I have no doubt that when Congress passed CALEA no one intended to create a situation of discrimination within our industry. But unfortunately, that's exactly what's happened. This committee holds the key to changing that. Make CALEA fair and make equitable. Help us in our efforts to help law enforcement, while at the same time ensuring that the personal communications services remain an integral part of an ever-growing and evermore competitive wireless industry. Thank you again for holding this hearing and the opportunity to testify and I look forward to working with this committee, with the FBI, to work on this in the future and I'd be happy to answer any questions you might have.

[The prepared statement of Mr. Kitchen follows:]

PREPARED STATEMENT OF JAY KITCHEN, PRESIDENT, PERSONAL COMMUNICATIONS  
INDUSTRY ASSOCIATION

SUMMARY

PCIA is the international trade association created to represent the interests of both the commercial and the private mobile radio service communications industries. As such, many of its members are providers of personal communications services ("PCS"), which is a type of broadband commercial mobile radio service that was intended to, and does, compete directly with cellular telephony.

Ever since the enactment of the Communications Assistance For Law Enforcement Act ("CALEA") on October 25, 1994, PCIA has played an important role in the statute's implementation. Specifically, PCIA has: (1) met with the FBI and its CALEA Implementation Unit ("CIU") in an effort to explain the unique difficulties the wireless industry in general, and the PCS industry in particular, have had in implementing CALEA; (2) taken an active part in the FBI's notice and comment rulemakings that implemented various sections of CALEA; and (3) sponsored many meetings that brought wireless carriers and manufacturers together in order to attempt to promulgate technical standards for CALEA-compliant network equipment.

Further, even as CALEA is being implemented, PCIA's member carriers have continued to cooperate with law enforcement officials in executing legitimate electronic surveillance warrants. This cooperation stems not just from their statutory obligation to do so, but from a recognition on the part of wireless carriers that the public safety is significantly advanced by the appropriate use of electronic surveillance techniques.

Against this background, PCIA offers its perspective on two of CALEA's most important requirements: the assistance capability requirements of Section 103, under which networks must be accessible to authorized wire tapping, and the capacity requirements of Section 104, under which a specific number of circuits must be reserved for law enforcement use. First, because technical standards for CALEA-compliant network equipment have yet to be promulgated, manufacturers cannot build this equipment, and carriers cannot purchase and install it. Therefore, Congress should amend CALEA to set a date that is at least 24 months after the date such technical standards are promulgated for the date on which carriers must comply with the assistance capability requirements. In addition, all equipment installed or deployed before this deadline should be either deemed compliant or retrofitted at the government's expense.

Second, Congress should ensure that in setting capacity requirements, the FBI takes into account the presence of multiple wireless carriers within a market. Congress should further ensure that the FBI reduces the capacity requirements for wireless carriers, promulgates wireless capacity requirements on a county-by-county basis, and does not group call content intercepts with trap and trace devices when calculating the capacity requirements.

## I. INTRODUCTION AND SUMMARY

PCIA is the international trade association created to represent the interests of both the commercial and the private mobile radio service communications industries. As such, many of its members are providers of personal communications services ("PCS"), which is a type of broadband commercial mobile radio service that was intended to, and does, compete directly with cellular telephony.

Ever since the enactment of the Communications Assistance For Law Enforcement Act ("CALEA") on October 25, 1994, PCIA has played an important role in the statute's implementation. Specifically, PCIA has: (1) met with the FBI and its CALEA Implementation Unit ("CIU") in an effort to explain the unique difficulties the wireless industry in general, and the PCS industry in particular, have had in implementing CALEA; (2) taken an active part in the FBI's notice and comment rulemakings that implemented various sections of CALEA; and (3) sponsored many meetings that brought wireless carriers and manufacturers together in order to attempt to promulgate technical standards for CALEA-compliant network equipment.

Further, even as CALEA is being implemented, PCIA's member carriers have continued to cooperate with law enforcement officials in executing legitimate electronic surveillance warrants. This cooperation stems not just from their statutory obligation to do so, but from a recognition on the part of wireless carriers that the public safety is significantly advanced by the appropriate use of electronic surveillance techniques.

Against this background, PCIA offers its perspective on two of CALEA's most important requirements: the assistance capability requirements of Section 103, under which networks must be accessible to authorized wire tapping, and the capacity requirements of Section 104, under which a specific number of circuits must be reserved for law enforcement use. First, because technical standards for CALEA-compliant network equipment have yet to be promulgated, manufacturers cannot build this equipment, and carriers cannot purchase and install it. Therefore, Congress should amend CALEA to set a date that at least 24 months after the date such technical standards are promulgated for the date on which carriers must comply with the assistance capability requirements. In addition, all equipment installed or deployed before this deadline should be either deemed compliant or retrofitted at the government's expense.

Second, Congress should ensure that in setting capacity requirements, the FBI takes into account the presence of multiple wireless carriers within a market. Congress should further ensure that the FBI reduces the capacity requirements for wireless carriers, promulgates wireless capacity requirements on a county-by-county basis, and does not group call content intercepts with trap and trace devices when calculating the capacity requirements.

## II. WHILE CONGRESS BELIEVED THAT CALEA-COMPLIANT EQUIPMENT WOULD BE AVAILABLE SOON AFTER JANUARY 1, 1995, SUCH EQUIPMENT IS STILL UNAVAILABLE BECAUSE STANDARDS HAVE NOT YET BEEN AGREED UPON

Congress enacted CALEA in large part because the new, digital telecommunications networks have become increasingly resistant to wire-tapping efforts by law enforcement officials. Importantly, however, CALEA was not intended to expand the technical capabilities of law enforcement, but only to give them the same capabilities in the age of digital equipment as they had in the analog era.<sup>1</sup> Therefore, in order to ensure that law enforcement officials could continue to carry out legitimate electronic surveillance efforts, Congress required that pursuant to the "assistance capability requirements" of Section 103 of CALEA, each carrier's network must be designed in a manner that allows law enforcement officials to expeditiously isolate and intercept both call-content and call-identifying information.

Carriers cannot meet their statutory obligations to provide law enforcement officials with this information unless they have access to switching equipment that is CALEA-compliant. If manufacturers are to provide carriers with this compliant equipment, there must be industry-wide technical standards that they can follow in designing and building their switches.

In drafting CALEA, under Sections 106 and 107, Congress contemplated that carriers, manufacturers, and law enforcement officials, in cooperation with industry associations or standard-setting organizations would cooperate to develop technical standards. Manufacturers would then build switches to these standards, and, soon

<sup>1</sup>H.R. Rep. No. 103-827, at 22 (1994) ("[t]he FBI Director testified that the legislation was intended to preserve the status quo, that it was intended to provide law enforcement no more and no less access to information than it had in the past").

after January 1, 1995, carriers would be able purchase and install this CALEA-compliant equipment.

Thus, even if the process worked exactly as planned, a carrier's ability to comply with CALEA would depend upon the ability and willingness of industry representatives and the FBI to reach a timely consensus on standards, and manufacturers' ability and willingness to manufacture compliant equipment in a timely fashion. Carriers would, however, as the entities responsible for ensuring that their networks are CALEA-compliant, be left "holding the bag" if this process broke down.

Unfortunately, a breakdown of monumental proportions has occurred. As of today, final standards have not been set, in large measure due to the actions of law enforcement officials. Initially, the FBI waited almost one and one-half years after the enactment of CALEA to submit its recommendations to standards setting bodies. After the submission of this list, industry representatives and the FBI were able to reach consensus on standards that provided, by PCIA's estimates, 90 percent of the capabilities that the FBI had requested. Since then, however, the FBI has held up the entire standards setting process in order to ensure that every capability on its "wish list" is made part of the standards.

This wish list consists of ten capabilities that most carriers believe to be either not required by CALEA, technically infeasible, or both. Thus, while carriers and manufacturers have acquiesced to virtually every law enforcement demand regarding CALEA capabilities, certain items of this "wish list" simply should not, and cannot be implemented. For example, the FBI has demanded timely, electronic notification of changes to a subject's feature capability that may prevent the delivery of intercepted communications, and separated delivery of content for each party in a multiparty call.

This continued delay is irrational and disserves the public interest. Law enforcement officials would have most of the capabilities they need if the proposed standards currently agreed upon by all parties were adopted today and the wish list items were deferred. Time is of the essence, because as carriers build out and upgrade their networks, they are buying new switching equipment. If this equipment were CALEA-compliant even if that term does not include the wish list items then law enforcement officials would be able to carry out most of their legitimate electronic surveillance missions. Otherwise, more and more networks will be built to non-CALEA specifications and will have to be retrofitted to comply with the state's requirements.

Further, this lack of agreed upon standards, and the consequential lack of CALEA-compliant equipment, threatens carriers with civil sanctions. Specifically, carriers whose networks do not comply with the assistance capability requirements by October 25, 1998 just one year from today can be fined up to \$10,000 a day.<sup>2</sup>

Therefore, the compliance deadline for the assistance capability requirements should be changed from October 25, 1998 to the date that is at least 24 months from the date that CALEA technical standards are approved. Because it takes a minimum of 24 months from the time a technical standard is promulgated until equipment based on that standard can be mass produced, such an adjustment will allow carriers to purchase and install CALEA-compliant equipment within the statutory deadline.

### III. THE LACK OF CALEA-COMPLIANT EQUIPMENT, AND COMPETITIVE CONCERNS, INDICATE THAT CONGRESS SHOULD ADJUST ITS REIMBURSEMENT AND GRANDFATHERING POLICY

Section 109 of CALEA distinguishes between network equipment that was installed or deployed before January 1, 1995, and network equipment that was installed or deployed after that date. Specifically, the Attorney General is commanded to either reimburse carriers for making their pre-1995 equipment CALEA-compliant or deem that equipment to be in compliance (*i.e.*, grandfather it).<sup>3</sup> For post-1995 equipment, however, carriers are responsible for paying the costs of ensuring

<sup>2</sup> 18 U.S.C. § 2522(c)(2).

<sup>3</sup> See 47 U.S.C. § 1008(a). The legislative history for CALEA further provides "[i]n recognition of the fact that some existing equipment, services or features will have to be retrofitted, the legislation provides that the Federal government will pay carriers for just and reasonable costs incurred in modifying existing equipment, services or features to comply with the capability requirements. The legislation also provides that the government will pay for expansions in capacity to accommodate law enforcement needs." H.R. No. 103-827, 103rd Cong., 2d Sess. 1, 10, 1994 U.S.C.C.A.N. 3489, 3490; see also *id* at 19, 1994 U.S.C.C.A.N. at 3499 (government is to pay the "reasonable costs incurred by industry in retrofitting facilities to correct existing problems.").

CALEA-compliance. Implicit in this statutory scheme is the *commercial availability of CALEA-compliant equipment* soon after January 1, 1995.

The aforementioned failure to reach an agreement on standards and the consequential failure of manufacturers to produce CALEA-compliant equipment has blown a huge hole in this statutory scheme. As a result of this failure, new carriers, such as providers of personal communications services, are placed in a financial bind. First, they must construct their entire networks from scratch at great expense. Then, when CALEA-compliant equipment becomes available, they will have to retrofit their networks to make them CALEA-compliant again, at great expense.

Established carriers, on the other hand, will be reimbursed for whatever retrofitting expenses they incur, thereby placing them at a competitive advantage relative to new carriers. These competitive inequities will be particularly acute for PCS providers, which have post-1995 networks, as compared to cellular providers, which have pre-1995 networks. While both entities will be selling a similar product, broadband wireless communications services PCS providers will have the additional, and substantial expense of making their networks CALEA-compliant, thereby placing them at a competitive disadvantage.

Congress should act to ensure that PCS providers which will provide cellular carriers with much needed competition are permitted to compete on a level regulatory playing field. Ensuring such regulatory parity will allow the carriers that provide the best combination of price, features, quality, and service to triumph in the marketplace rather than pre-ordaining the result by asymmetric regulation.

The best way to level the regulatory playing field is to change CALEA's reimbursement policy so that any network equipment that is installed or deployed before CALEA-compliant equipment is commercially available is either deemed to be in compliance or eligible for reimbursement. Such an amendment will also fulfill Congress's original intent in enacting CALEA that individual carriers not be required to pay retrofitting costs that should rightfully be borne by the government.

One way in which an equipment retrofit can be accomplished in a cost-effective manner is through the development of software upgrades for all switches, whether they were manufactured before or after 1995. PCIA is currently working with the FBI and switch manufacturers to develop a program whereby the FBI uses the monies allocated under Section 110 for the retrofitting of pre-1995 equipment to contract for the development and distribution of this software. Congress should, however, be aware that the Section 110 authorization is only for the years 1995 through 1998, and might consider extending that authorization.

Finally, in order to make this software upgrade program consistent with the language of CALEA, Congress must amend Section 109(a) to allow the Attorney General to pay telecommunications carriers and *telecommunications equipment manufacturers* for the costs of making both their pre-1995 equipment and their *post-1995 equipment* CALEA-compliant. These statutory changes will allow carriers, manufacturers and the FBI to proceed with a program that represents the fastest and most efficient means of bringing all of the nation's switches into CALEA compliance.

### III. THE CAPACITY REQUIREMENTS FOR WIRELESS CARRIERS ARE TECHNICALLY DEFICIENT AND SHOULD BE ALTERED

In its *Second Capacity Notice*, pursuant to Section 104 of CALEA, the FBI mandated actual and maximum capacities or the number of circuits that must be reserved for law enforcement use for both wireline and wireless carriers. The capacity requirements for wireline carriers were mandated by county, while the capacity requirements for wireless carriers were mandated by wireless service area, including Metropolitan Statistical Areas ("MSAs") and Rural Statistical Areas ("RSAs") for cellular carriers, and Major Trading Areas ("MTAs") and Basic Trading Areas ("BTAs") for PCS carriers. While the wireline capacity requirements were based on the historic number of landline wiretaps, the wireless capacity requirements were based on the historic number of cellular wiretaps.

In light of the large size of the wireless service areas used by the Bureau and the amount of competition in the wireless market, the proposed capacity requirements for wireless carriers are excessive. Initially, the FBI should not extrapolate the capacity requirements for an entire MTA based on a single metropolitan area, as this requires carriers to substantially overbuild their capacities. For example, in the New York MTA, only New York City and its suburbs (*i.e.*, the New York BTA) require a significant number of intercepts. Nevertheless, carriers serving this MTA must build the capacity necessary to meet the law enforcement needs of the New York metropolitan area into their entire networks which extend from New Jersey to Vermont.

Further, at present, local wireline telephone companies do not face a great deal of competition in their markets, if any at all. Wireless telephony, on the other hand, is subject to vigorous competition, as two cellular providers compete with up to six broadband PCS operators in each market. Given this level of competition, it is unreasonable to assume that every conversation that law enforcement officials wish to monitor is being carried over a single provider's network. Yet, by requiring each wireless carrier in a given service area to meet the actual and maximum capacities in their entirety, the FBI implicitly makes this assumption.

While it is unrealistic to expect the FBI to apportion capacity requirements precisely by market share, it is unfair and wasteful of resources to require every carrier to meet the actual and maximum capacity requirements in their entirety. Thus, in areas where there are multiple wireless carriers, the FBI should spread the capacity requirements over all of these carriers. Similarly, because new carriers will have many fewer customers than established carriers, these new entrants should be required to engineer less wiretapping capacity into their networks.

The large size of wireless service areas and the amount of wireless competition points to the fact that wireless capacity requirements should be made more granular, and the number of wireless carriers per county should be factored into these capacity requirements. This could be accomplished if wireless capacities, like wireline capacities, were promulgated on a countywide basis and service area capacities for wireless carriers were calculated as  $(1/\text{number carriers in the service area}) \times (\text{the capacity of the most wiretapped county in the service area})$ .

Finally, the FBI admits that historically, there have been a "vastly greater number" of call identifying intercepts (pen register and trap and trace) than Title III (call content) intercepts. However, in setting forth capacity requirements, the FBI did not distinguish between these differing types of intercepts. Because the technologies—and the cost—required to support these different types of electronic surveillance varies widely, the FBI should promulgate separate requirements for call content, trap and trace, and pen register intercepts. This distinction will make it significantly easier for carriers to comply with the FBI's requests without engineering more of any single type of capacity into their networks than is necessary.

### III. CONCLUSION

Congress should take this opportunity to fine tune CALEA's compliance deadlines and reimbursement programs to make them more reflective of the technological and competitive realities of the telecommunications industry. Such adjustments will provide a competitively neutral, cost effective method by which the FBI, telecommunications carriers, and switch manufacturers can make all of the nation's switches CALEA-compliant. This upgraded infrastructure will, in turn, give law enforcement officials the electronic surveillance capabilities they need to assist them in solving and preventing criminal activity. I thank the Chairman and the Committee for conducting this hearing and look forward to working with the Committee to amend the statute so that it is fair to all players and does not disproportionately burden new entrants.

Mr. McCOLLUM. Thank you very much, Mr. Kitchen.

Mr. Neel, welcome and you may proceed to give us your summary.

### STATEMENT OF ROY M. NEEL, PRESIDENT, U.S. TELEPHONE ASSOCIATION

Mr. NEEL. Thank you, Mr. Chairman, and we do appreciate your interest in this issue and that of your colleagues. We are stuck in a ditch here, as you're hearing. There have been ongoing negotiations and some very positive signs and we're all hopeful that this will be resolved. But there are some bones of contention that you should take into consideration as you're looking at reasons why we're in this ditch.

To back up just a little bit, we believe, all the nation's local carriers, that the intent of this act in 1994 was to grandfather, or to make in compliance, all existing equipment. There was considerable debate about this and law enforcement agreed. As Tom mentioned, we sat here and we advocated the passage of this act, be-

cause we believed there was an understanding that existing equipment be grandfathered. The cost of retrofitting existing equipment would be astronomical, absolutely astronomical. So we had that understanding. The agreement was that the industry would develop for the future technologies with wiretap capabilities which are reasonably available. And the Act states that the industry would develop the technical standards not law enforcement, the FBI or whomever, would decide on the standards and hand them over unilaterally to industry. So we're stuck in a ditch there if law enforcement essentially has a veto over any industry standards that were developed. And we've been working very hard over the last few years to do just that.

A third issue is critical to all of us who have to build and maintain networks and pass on costs to our rate-payers. Because much of this is not just about the impact on the owners of our businesses, whether they're mom and pops, and we have a thousand of those, by the way, or whether they're very large businesses. We have to pass these costs on to customers if we're allowed to be regulators. In our case, consumers of basic local telephone service may well end up paying.

We are also in an extremely competitive environment, so none of our companies represented here today has the option even of just absorbing these costs. So there's a dispute about who pays and when. Basically, there are a couple of issues. One is whether or not our industry or our companies will be reimbursed for upgrading our network equipment installed or displayed after January 1995.

Also, there is, very honestly, a disagreement about what it's going to cost to meet the requirements that have been proposed by law enforcement, by the FBI, by the technicians, as Tom indicated, in these agencies. We don't believe that this is a small issue. You have authorized a considerable amount of money under this act to make this happen. And as Mr. Meehan said, none of this money has been drawn down, and he's correct. But our assessment of what law enforcement is requesting or demanding in this process is far in excess of the money you've made available. We're not here calling for you to authorize or appropriate more money, but we would like to bring a reasonable assessment to this.

Let me just give you an example. There's 500 million dollars that's been authorized, as I said, to bring these platforms into compliance. We canvassed three of the major switch manufacturers, that cover roughly 75 percent of the market, but not all of it, and that other 25 percent is critical. We asked them what would it cost to meet law enforcement's demands here. No prejudice about the amount, we have no incentive to balloon the amount, we're forced to be conservative here. And what we found out was this. That to meet the compliance standards that we all agree to here, as Tom mentioned, under the industry-proposed standards, it could cost between 240 and 620 million dollars just for those baseline standards that we all agree to. But to meet the requirements that law enforcement has called for, a so-called punch list, you may have heard that term in these discussions, could cost an additional 217 to 602 million dollars. So that comes out to about 450 million to 1.2 billion dollars to do simply this -to bring three of the major wire line switches, this doesn't cover Tom or Jay's enterprises, only

three of those switches into compliance, could cost up to 1.2 billion dollars.

Now, we believe that there is a serious problem here. And if we don't resolve this issue we may not only risk liability for non-compliance, but could be threatened with huge fines and penalties. Moreover, we could be threatened with having to swallow those costs and none of us wants to hire lawyers, frankly, to go litigate these things.

So this is just a portion of what we believe this is going to cost. And we're not asking for you to appropriate 1.2 billion dollars. I mean, frankly, whatever the Government spends to upgrade these networks, to make them compliant with CALEA, may not be enough. Our companies may have to absorb some of these costs, the Government is, as well. But it's important to keep those reasonable, because the act is very specific about this. It says that the industry would develop these technologies with wiretap capabilities that are reasonably achievable. So we think that law enforcement has to take all of these things into consideration.

So, I want to summarize briefly what we are asking law enforcement to do. By the way, the local telephone industry is not asking for a rewrite of CALEA. We think the law was a good one. We all worked on it for years. We were here with you. This goes way back even into the Bush administration, as you know, so there's a lot of hard work that went into this law. So we believe that law enforcement must agree that existing equipment is deemed in compliance, that safe harbor standards need to be adopted right away, without further delay, and, as part of that, the law enforcement has to move back the compliance date, the October 1998 date, which is—regardless of cost—if you appropriated and they had 10 billion dollars in their pocket—impossible to meet. Because the standards aren't out there and it takes longer than that for the manufacturers to do their work and then to get it into the networks. And we don't want to face those lawsuits and fines, either.

So let's get the job done now. We've been working hard on this. We think that law enforcement is negotiating in good faith, but there are, in all honesty, some serious problems down in that ditch. Thank you, Mr. Chairman.

[The prepared statement of Mr. Neel follows:]

PREPARED STATEMENT OF ROY M. NEEL, PRESIDENT, U.S. TELEPHONE ASSOCIATION

#### SUMMARY

Telecommunications carriers are proud of the role they play in assisting law enforcement agencies execute legally authorized electronic surveillance. The more than 1,100 local exchange carriers of USTA look forward to continued cooperation with law enforcement in this regard, and to the successful implementation of CALEA. Meanwhile, it should be recognized that more wiretaps are being conducted every year, using existing network (i.e., non-CALEA) technology.

CALEA provides a four to six year transition period following enactment, during which new CALEA-based wiretap capacities and capabilities would be developed for deployment in future telecommunications networks during carriers' normal course of business.

Three years after enactment, CALEA's implementation is not on track. A notice of capacity requirements, expected one year after enactment, has yet to be issued. Safe harbor standards describing technical capabilities that manufacturers need to develop CALEA solutions have not been adopted. Nowhere in CALEA is there a requirement that carriers retrofit existing equipment; yet, cost reimbursement rules cast doubt on the government's intent to reimburse carriers for their reasonable

costs of retrofitting existing network facilities. Finally, because it will take between 18 to 30 months to develop CALEA software and hardware solutions, CALEA's compliance date of October 25, 1998 (subject to requests for up to a two year extension), is now impossible to meet.

USTA believes that implementation of CALEA can be put back on track by concurrently resolving capability, cost reimbursement, compliance date and capacity issues. USTA therefore proposes the following recommendations:

1. *CALEA should be clarified to remove any doubt that existing network equipment is deemed in compliance with CALEA until CALEA-based technical solutions are available for installation in carriers' networks.*

CALEA provides that any facilities "installed or deployed" after January 1, 1995 must be reasonably achievable. However, equipment deployed today is equally as non-CALEA compliant as equipment deployed in 1994. Existing network facilities cannot be considered reasonably achievable since CALEA technology is not yet available. Such equipment therefore should be deemed in compliance. If it is not, carriers would be forced to seek individual determinations of reasonable achievability, or seek court remedies, both of which will only further add unnecessary delay and expense of implementing of CALEA.

2. *Safe harbor industry standards must be allowed to be adopted.*

Industry standards-setting bodies, in consultation with law enforcement, have proposed technical standards that USTA contends are 100 percent CALEA-compliant. Law enforcement has insisted that these standards should include additional items (i.e., the so-called "punch list") that industry and privacy organizations contend are either unnecessary or may exceed the scope of the law. There are other means to address punch list items. Any further opposition by law enforcement to the proposed industry standards will further delay their availability to manufacturers, preventing timely deployment of new CALEA-based upgrades in the nation's networks.

3. *CALEA's compliance date (10/25/98) should be moved to enable sufficient time in which to install CALEA solutions in carriers' networks.*

While CALEA allows carriers to request from the FCC extensions of this deadline, the FCC could be inundated with such requests from thousands of carriers, serving tens of thousands of facilities and services for which an extension would be required. Instead, since implementation has taken longer than anticipated when CALEA was drafted, and compliance by 1998 therefore is not reasonably achievable, the compliance date should be moved.

4. *Capacity requirements must be issued before carriers are able to fulfill both their capacity and capability obligations.*

Capacity requirements must be consistent with historic electronic surveillance trends and must provide sufficient technical description to enable carriers and manufacturers to develop and install compliant hardware and software solutions.

In conclusion, telecommunications carriers look forward to continuing to work with law enforcement agencies in executing legally authorized electronic surveillance. While existing telecommunications facilities are providing electronic surveillance capabilities for law enforcement purposes, the industry recognizes its responsibilities to design, develop and install surveillance capabilities as specified in CALEA. It is essential, however, in making the transition from present network facilities to future CALEA-compliant networks, that carriers are allowed to modernize their networks without CALEA coming back to haunt these carriers and their customers with potentially hundreds of millions of dollars of retrofitting expenses.

Representatives of industry and the Department of Justice have been discussing these implementation issues with a goal of removing obstacles to timely implementation of CALEA. We look forward to continuing these discussions, and to working with Congress to remove the clouds of uncertainty that threaten implementation of CALEA with the unnecessary expense and delay of pursuing regulatory and/or court remedies. We remain confident that CALEA can be implemented in a timely and reasonable fashion that protects law enforcement, industry, and privacy interests as Congress intended when passing CALEA in 1994.

#### INTRODUCTION:

It is an honor to appear again before this committee to discuss the Communications Assistance for Law Enforcement Act (CALEA). The last time I was here on this matter was over three years ago, when I testified along with my colleague here from CTIA, Tom Wheeler, and FBI Director, Louis Freeh.

USTA represents 1,100 wireline local exchange companies throughout the United States. Some of our member companies are among the largest corporations in the country, such as Bell Atlantic and BellSouth. We also represent dozens of mid-sized companies like Cincinnati Bell, ALLTEL, TDS, and Denver and Ephrata Telephone Company in Pennsylvania. The vast majority of our members are small, rural, family-owned businesses or telephone cooperatives, owned by their customers, such as Randolph Valley Telephone Cooperative in North Carolina, Lavaca Telephone Company in Arkansas, and Pulaski-White Telephone Cooperative in Indiana.

USTA member companies represent over 95% of all the telephone access lines in the country. And while our small company members serve only 3 percent of the U.S. population, their service territories cover over 40% of the country's land mass. Moreover, roughly 50% of the nearly 26,000 wireline telephone switches (the computers responsible for routing calls throughout the network) in the country are operated by these smaller companies; so while most access lines in the nation are served by a few companies, most switches in the country are operated by hundreds of small companies. This is important in understanding the potential ramifications of CALEA's implementation on telephone companies.

It must be pointed out that every one of these telephone companies has, and will continue to cooperate with law enforcement agencies in assisting them to perform properly authorized electronic surveillances. In fact, law enforcement has not divulged a single instance to us where a wireline carrier has not been able to perform a court ordered surveillance. As the annual report of the Administrative Office of the U.S. Courts indicates, more wiretaps are being conducted than ever before. It should be noted that this growth is taking place on *today's existing network facilities*. We are proud to do our part to assist in the many successful prosecutions the FBI and other law enforcement agencies have made using legally authorized wiretaps, traps and traces, and pen register information provided by telephone companies.

#### *1994: CALEA's Balance of Priorities*

CALEA represents a careful balance between law enforcement, industry, and American citizens' Constitutional rights to privacy and freedom from government intrusion. CALEA provides both safeguards and obligations for each of these interests.

For law enforcement, CALEA grants for the first time in our history, a statutory requirement that industry will design electronic surveillance capabilities for future telecommunications network equipment. (47 USC 1002.) The Attorney General also is granted enforcement authority, including the power to seek \$10,000 a day penalties for non-compliance. (18 USC 2522.)

Industry's obligations are to design and develop electronic surveillance capabilities and capacities for future network-deployed facilities. (47 USC 1002.) However, realizing that it is punitive to require retrofitting of existing network technologies with CALEA technology that has not yet been developed, CALEA protects existing network facilities (i.e., those installed or deployed prior to January 1, 1995) by deeming them in compliance with the law, unless the government reimburses the carrier to bring them into compliance, or unless they are replaced or "significantly upgraded" or modified by the carrier. Equipment deployed after January 1, 1995 is subject to a determination by the Federal Communications Commission of whether compliance is "reasonably achievable." (47 USC 1008.) In short, industry would deploy—at industry expense—reasonably achievable CALEA technology solutions after they become available, while *existing* facilities were to be grandfathered unless the government pays for bringing facilities it identifies into compliance.

CALEA also grants specifically to industry the authority to develop technical standards which provide a safe harbor to carriers and manufacturers that install or deploy equipment which complies with such standards. (47 USC 1006.) While the Attorney General may consult with the industry standards-setting bodies, the government may not impose any design specifications. (47 USC 1002.) Further, even as CALEA requires industry to develop CALEA capabilities for future deployments in their networks, it provides a standard of reasonable achievability. This means that if compliance cannot be reasonably achieved, a carrier may nevertheless deploy facilities and such facilities would be deemed in compliance with CALEA. (47 USC 1002, 1008.) CALEA also provides protections against enforcement orders when compliance is not reasonably achievable with available technology. (47 USC 1008.) Finally, CALEA grants the ability to seek from the Federal Communications Commission extensions of compliance deadlines under various circumstances. (47 USC 1006.)

Individuals' rights to privacy and protection from government intrusion are protected as well. CALEA specifically requires the development of surveillance capabilities that protect the privacy and security of communications not authorized to be

intercepted. (47 USC 1002, 1006, 1008.) CALEA's legislative history also clearly states that the law is intended to be narrowly interpreted by industry and law enforcement and the FCC to preserve, and not expand, surveillance authority. Further, CALEA grants the ability to any individual to petition the FCC if technical standards are deemed deficient. (47 USC 1006.)

*1997: Implementation Off Balance and Delayed*

*1. Cost Reimbursement and Reasonable Achievability During the Transition Period*

Since it has taken longer than anticipated in 1994 to develop both capacity and capability requirements, the conditions that existed when CALEA was enacted have not changed. Existing equipment in 1997 is equally as non-CALEA capable as it was in 1994. (It also is equally as capable of providing electronic surveillance as it was in 1994 too, albeit in a non-CALEA manner.) Nowhere in CALEA is there a requirement that carriers must "retrofit" existing equipment. Nonetheless, the FBI is threatening carriers with the possibility of having to go back into their networks and retrofit them with potentially extremely expensive CALEA upgrades, contrary to the intent of CALEA.

In March, 1997, the FBI adopted rules for CALEA cost reimbursement. Most significantly, the rules fail to differentiate between the terms, "installed or deployed," as required by CALEA. Instead, the rules dictate that the costs of modifying or retrofitting only such equipment that has been "installed" prior to January 1, 1995 may be eligible for reimbursement. Any equipment, features or services placed in service after January 1, 1995—according to the FBI's interpretation—would be the carrier's responsibility to retrofit, potentially at tremendous cost to the carrier and its customers. The rules, in short, attempt to force carriers, in contravention of CALEA, to retrofit existing equipment.

CALEA states that the government will reimburse carriers to bring into compliance such embedded-base equipment it needs to retrofit during the four-to-six-year transition period following enactment. Indeed, the legislative history states:

The bill requires the Federal government, with appropriated funds, to pay all reasonable costs incurred by industry over the next four years to retrofit existing facilities . . . In the event that the \$500 million [authorized] is not enough or is not appropriated, the legislation provides that any equipment, features or services deployed on the date of enactment, which government does not pay to retrofit, shall be considered in compliance until the equipment, feature, or service is replaced or significantly upgraded or otherwise undergoes major modification.

After the four year transition period, which may be extended an additional two years . . . industry will bear the cost of ensuring that new equipment and services meet the legislated requirements, as defined by standards and specifications promulgated by the industry itself. (H. Rept. 103-827, p.16.)

A four-to-six-year transition period was provided to enable the development of CALEA technology while carriers continue to modernize their networks to meet increasingly competitive market forces. The transition period was intended to protect not only equipment already installed by 1995, but equipment "in the pipeline," (i.e., equipment already designed, developed, and utilized in the industry, but not yet installed). Both the statute and legislative history assure that "if a service or technology cannot reasonably be brought into compliance with the interception requirements, then the service or technology can be deployed." (H.Rept.103-827, p.19.) The four/six year transition period and the Act's provisions allowing for continued deployment of network facilities therefore were intended to assure carriers that their networks would be deemed compliant with CALEA unless the government reimbursed the carrier to bring certain facilities into compliance with CALEA. After CALEA-compliant technology becomes available, the carrier would be required to deploy only CALEA-compliant equipment, facilities and services in the ordinary course of performing network upgrades.

Because of delays in implementing CALEA, there is no difference between a switch being installed or deployed today and a switch installed or deployed prior to January 1, 1995. Both would be deemed in compliance with CALEA. The pre-1995-installed switch would be deemed in compliance because it was installed prior to January 1, 1995. The post-1995-installed switch would be deemed in compliance because compliance is not reasonably achievable; and in any event, the switch had been deployed in the network. Among the factors the FCC is required to consider in determining reasonable achievability are cost to the carrier and its customers, and the extent to which such equipment is designed or developed prior to January 1, 1995. (47 USC 1008.) While one switch was "installed" prior to January 1, 1995,

the other was "deployed" (i.e., designed and developed) prior to January 1, 1995. USTA believes that Congress specifically used the words, "installed or deployed" (not "installed *and* deployed") to capture this distinction.

Thus, USTA contends that CALEA intended to treat such equipment installed or deployed since January 1, 1995, and prior to the availability of CALEA solutions (assumed at the time to be four to six years hence) as not reasonably achievable. Such equipment would be deemed in compliance with CALEA, unless the government reimbursed the carrier to bring it into compliance. Any other interpretation would force carriers to seek individual determinations of reasonable achievability from the FCC during the transition period for "any equipment, facility, or service installed or deployed after January 1, 1995." This would inundate the FCC with requests for determining reasonable achievability; cost carriers both time and expense in pursuing regulatory remedies; and delay even further the implementation of CALEA.

Moreover, if the FCC were to determine that carriers must retrofit post-1995 installed or deployed equipment at their own expense—despite the fact that nothing in CALEA requires carriers to retrofit equipment—a Constitutional challenge could be initiated on the grounds that forcing carriers to provide a government service without reimbursement constitutes unlawful taking under the Fifth Amendment. This only adds to the prospects of additional expense and further implementation delay.

### *2. Significant Upgrades and Major Modifications*

The FBI sought comments last year on the definition of the terms, "significant upgrade" and "major modification." A final definition has not yet been proposed. However, USTA and many others have expressed their concerns, based on the FBI's comments at industry meetings and its reimbursement rules, that a narrow interpretation of these terms will only further threaten inappropriately to shift costs to carriers, and effectively force retroactive, ubiquitous retrofitting of the nation's telecommunications infrastructure, contrary to the intent of CALEA and in contradiction of comments made by FBI Director Freeh before this Committee in 1994.

Mr. Neel mentioned that the passage of the statute and enactment of these mechanisms would be an invitation for the ubiquitous use . . . of wiretaps. I think that this is just not valid . . . We do not propose . . . rewiring America . . . (FBI Director, Louis Freeh, at Joint Hearings of the House and Senate Judiciary Committees, August 11, 1994.)

CALEA is intended to grandfather embedded-base equipment that cannot have been installed or deployed with CALEA technology, since CALEA technology does not yet exist, unless the Attorney General agrees to reimburse the carrier to bring it into compliance. Also, CALEA intends to allow carriers to deploy facility modifications and upgrades without penalty.

Therefore, USTA believes the only practical definition of significant upgrade or major modification, consistent with the intent of the law, must allow for network modernizations to continue to be made prior to the availability of CALEA technology. In other words, existing telecommunication network facilities installed, deployed or modified prior to the availability of CALEA solutions must be deemed in compliance with CALEA. Upgrades or modifications to such existing equipment in the ordinary course of business, and prior to the availability of CALEA solutions cannot be considered "significant upgrade" or "major modification" for purposes of CALEA.

Carriers not only are installing new equipment in their networks regularly, they more frequently upgrade facilities, much as personal computer owners upgrade their word processing programs with the latest editions. With the enactment of the Telecommunications Act of 1996, competition has increased dramatically, requiring even more intensive, and frequent, modernization of telecommunications networks. Indeed, entirely new companies and technologies are being introduced in the telecommunications market. Since practically all telecommunications equipment at least has been upgraded with new software since 1995, the definitions of "significant upgrade" or "major modification" become extremely important. If these terms were defined to apply to any or all modifications or upgrades since 1995, virtually no equipment would be deemed in compliance, despite the fact that none of it can be considered reasonably achievable. All of it would be considered the carrier's responsibility to retrofit.

### *3. Capability Standards Are Not Available*

CALEA grants the authority to industry standards-setting bodies to develop standards which constitute a safe harbor for any manufacturer or carrier that builds

to or installs equipment that complies with the standard. (47 USC 1006.) It also prohibits the government from requiring any design specifications or the adoption of any particular features. (47 USC 1002.) Further, CALEA anticipates a four (to six, including a two year extension) year transition period during which it was assumed that standards would be developed and manufacturers would design and develop CALEA capabilities for installation in telephone networks.

All has not gone exactly as anticipated. Industry standards-setting bodies comprising of representatives of carriers and manufacturers, began drafting technical solutions even before CALEA was enacted. Industry also sought law enforcement suggestions concerning its interpretation of CALEA technical requirements. A final version of government recommendations was delivered to industry last Summer (1996) in a document called the Electronic Surveillance Interface (ESI). Through the Fall and Winter of last year, industry standards-setting bodies evaluated the ESI and worked with law enforcement to accommodate ESI recommendations.

After hundreds of meetings between law enforcement and industry, a proposed industry national standard, to be sanctioned by the American National Standards Institute (ANSI), was released for approval by interested parties earlier this Spring. However, law enforcement effectively prevented approval of this standard, claiming it did not go far enough in adopting all of the ESI's recommendations.

The industry standards represent a consensus among wireless and wireline carriers and manufacturers that comply 100% with CALEA. The proposed industry standards implement over 90% of the functionalities requested by the ESI, leaving only 11 items that law enforcement has identified (referred to as the "punch list," or by law enforcement as "missing capabilities") that are not included in the proposed industry standard. In some cases, "punch list" items may violate CALEA's clear protections of the privacy of communications not authorized to be intercepted, such as being able to listen in on a conference call even after the target has left the call. Other items on the punch list are not required by CALEA. They do not pertain to the isolation and delivery of call content or call identifying information. Many of these present serious technical feasibility issues. An example is the ability to deliver automatically and immediately notification to law enforcement of a change in services provided by a surveillance target when other, less expensive alternatives are available. Other examples include notification of specific buttons pushed on a telephone handset, or delivery of certain information within a half-second, which is faster than many switches deliver such data. These items, while possibly desirable for law enforcement to obtain, would be expensive, and expensive, to develop and install. As such, the punch list imposes additional technical requirements and potentially significant, unnecessary costs on carriers and their customers.

A second proposed ANSI-sanctioned industry standard is currently being circulated for ballot, with a deadline by the end of October. If law enforcement again attempts to defeat adoption of this proposed standard under ANSI rules, industry may adopt an interim standard of limited duration and subject to renewal and eventual ANSI approval. It is time to release a safe harbor standard, as CALEA intended, that manufacturers will be able to use in initiating the design and development of CALEA technologies.

In short, law enforcement has impeded the adoption of necessary standards by insisting that the ESI must be adopted by industry. The wireline industry has attempted to accommodate law enforcement in an effort to implement the law efficiently and to avoid protracted proceedings at the FCC. Thus, despite CALEA's clear prohibition against government design of capabilities, law enforcement's management of the implementation process effectively is requiring specific designs or system configurations to be adopted by industry, resulting in continued delay in releasing an industry standard.

#### *4. Capacity Notices Are Not Available*

CALEA requires the Attorney General to issue a notice of capacity requirements to industry not later than one year after enactment, (i.e., by October 25, 1995). (47 USC 1003.) Carriers would have three years after notification by the Attorney General to install capacity that meets the notification requirements. It is now three years after enactment, and a final capacity notice has yet to be issued. The first two proposed notices issued by the FBI have met with widespread criticism. USTA's comments to the FBI pointed out that the proposed notices both were: 1) expansive, requiring far more capacity than can be historically justified—a potential waste of taxpayer money; and, 2) technically deficient, failing to provide carriers with the type of technical information about channel requirements, different types of surveillance activity required (e.g., trap and trace, pen register, or call content), or interface delivery requirements which carriers need to be able adequately to engineer capacity loads in their networks. We understand that law enforcement is nearing com-

pletion of a third notice. We hope our suggestions, and those of many other commenters, will be adopted in this latest version.

#### *Costs of CALEA Compliance Call for Law Enforcement Prioritization*

CALEA authorizes \$500 million, subject to appropriation, for law enforcement to use in bringing existing equipment into compliance with CALEA. USTA argued that depending on design requirements, retrofitting the nation's telephone network would cost more like \$2 billion, a figure we believe remains accurate today, as more information comes in from manufacturers now able to provide estimates based on the proposed industry standard. Thus, CALEA requires law enforcement to identify such facilities it determines warrant upgrades, and to prioritize its spending to upgrade those facilities most in need of modification. We continue to believe that \$500 million is not enough to retrofit existing facilities, given what we currently know about developing switched based solutions conforming to proposed industry standards.

In submitting its Implementation Plan to the House and Senate Appropriations and Judiciary Committees earlier this year, pursuant to the FY97 Appropriations Act, the FBI simply states that there are 35 switching platforms in use today in wireline and wireless networks, 19 of which it describes as "priority switching platforms," representing 97 percent of all wireline and 96 percent of all wireless interceptions.

Three major wireline switching platforms (the Lucent 5ESS, Siemens EWSD, and Nortel DMS100) deployed today account for roughly three-quarters of all the access lines in use in the nation's wireline network. One large carrier wireline representing several high surveillance activity areas in the U.S. deploys nearly 100% of its access lines with these three switches. However, the percentage of lines served by these switches decreases particularly with USTA's smaller member companies where a wider variety of switches and switch manufacturers are found. Given the cost of developing CALEA software solutions for just these three switches (see below), the FBI needs to consider the diminishing marginal returns of retrofitting more platforms. Also, many of the other switching platforms in the embedded telecommunications network base are older generation switching platforms that do not require the same level of technical solution for electronic surveillance.

Price estimates supplied by equipment manufacturers indicate that software development only for the three "major" wireline platforms will be between a low of \$240 and a high of \$620 million. This range represents only the cost of software development of those capabilities contained in the proposed industry standard. It assumes manufacturers' discounted prices for a single, nation-wide software solution. It does not include the cost of wireline software development of any "punch list" items, which estimates predict would cost an additional \$217 to \$602 million. It does not include any wireless technology solutions. This estimate further does not include additional costs incurred by carriers to test, engineer, and install CALEA software in their existing networks. These costs are estimated to range between \$150 million and \$200 million. Further, CALEA upgrades may often require carriers to purchase and install additional hardware to preserve switch processing capacity and maintain network integrity. This estimate does not include any of these related hardware costs directly associated with CALEA implementation. The estimate also does not include any capacity related costs.

The need for prioritization was emphasized by Director Freeh during the August, 1994 hearings before this Committee:

So I would take issue with the idea that this is going to spawn more wiretaps simply by the use of capability and access and that I think we have a pretty good idea where we need to build to protect . . . [If Congress] made a finding that . . . the money stops[,] I would still be in a better place if I could have access to half of the criminal conversations than none of the criminal conversations . . . I think over a long-term period, if . . . we are talking now about designing switches for 1998 and 1999, it seems to me that there will be a much more expansive benefit and a permeating benefit by starting early, particularly with the larger systems which will work to the benefit of upgrading the smaller systems.

In short, the assumption in 1994 was that development of CALEA solutions was a long term process, that would focus on higher priority, larger systems first, and that it would not seek 100% near-term ubiquitous capability. Given the implementation delays and problems that have been encountered, a 1998-1999 switch deployment time frame now appears to have been a highly ambitious assumption. However, the recognition of CALEA as a process and the Director's tone of reasonableness is as appropriate today as it was in 1994.

Moreover, the fact that the \$500 million may be spent on software development only, and only on the three major wireline switching platforms currently deployed, further illustrates two additional concerns. First, the effects of CALEA may be disproportionately burdensome on small telephone carriers. It is these carriers who more frequently, although not exclusively, deploy a variety of switches other than the 5ESS, EWSD or DMS100. Second, if CALEA solutions are reimbursed for the three major platforms, but not for the others currently deployed, CALEA in effect could create a dichotomy between those carriers who would receive "free" CALEA upgrades whose development and installation costs are reimbursed by the government, and those who do not. The latter certainly would seek a determination from the FCC that compliance is not reasonably achievable.

*Compliance Date (October 25, 1998) is Now Impossible to Meet:*

Given the fact that industry safe harbor standards will not be available until late 1997, the October, 1998 compliance date is impossible to meet. CALEA grants the authority to the FCC to grant an extension of the compliance date for any "facility, service or feature" for up to two years. There are over 26,000 wireline switches alone in the country. These switches each deploy a wide variety of services or features. Clearly, compliance is not reasonably achievable, and an extension of the compliance deadline for every facility, service or feature in the country would be appropriate. The FCC faces potentially thousands of requests for compliance deadline extensions. (Again, smaller telephone carriers may face an equal if not even greater burden in pursuing legal/regulatory remedies.)

*Time Line for Implementation*

If implementation is put back on track, we believe CALEA technology can begin to be deployed in the nation's telecommunications networks in a timely manner. Industry standards should be adopted in November, 1997. Manufacturers will then need 18 to 30 months to develop software solutions. Deployment in carrier networks, therefore, conceivably could begin between May, 1999 and May, 2000. Finally, the nation's major wireline carriers install routine software upgrades on their network facilities every six to 18 months. Thus, if law enforcement funds the development of solutions to bring existing equipment into compliance with CALEA, this technology could be deployed within 18 months of the CALEA solutions' availability during carriers' normal course of business upgrade deployment.

*USTA Recommendations to Put CALEA Back on Track*

USTA believes that implementation of CALEA can be put back on track simply by returning to the standard of reasonableness that prevailed during consideration and passage of CALEA three years ago. Because of the interrelationship between capability, cost reimbursement, capacity, and the compliance date, all four implementation issues must be resolved concurrently for implementation to proceed without further delay.

1. *CALEA's grandfather date should be clarified so that existing equipment (deployed, installed or upgraded since January, 1995) is deemed in compliance with CALEA until CALEA-based technical solutions are available for installation in carriers' networks and such equipment is retrofitted at government expense.*

The government may, based on its priorities and the availability of funds, reimburse carriers to bring currently-deployed equipment into compliance. However, currently deployed or installed facilities cannot be considered reasonably achievable since CALEA technology is not available; therefore, it should be deemed in compliance. If not deemed in compliance, carriers would be forced to seek individual determinations of reasonable achievability, or seek court remedies, both of which will only further delay implementation of CALEA.

2. *Safe harbor industry standards must be allowed to be adopted.*

Proposed industry standards have been drafted by industry standards setting bodies, in consultation with law enforcement, as provided for under CALEA. These proposed standards represent a consensus among manufacturers and carriers, and, but for a few items, adopt nearly all of law enforcement's recommendations. Industry stands by its proposed standards as 100 percent CALEA-compliant. Any further opposition to the proposed standards will only delay their availability to manufacturers, preventing timely deployment of new CALEA-based upgrades in the nation's networks. For those items not included in the proposed industry standard (i.e., the so-called "punch list," or "missing capabilities"), government may contract with carriers or manufacturers to develop and install such capabilities, to the extent they do not violate provisions

of CALEA or other legal principles. Moreover, CALEA provides that any person may petition the FCC if standards are deemed to be deficient. Further intervention in the standards process will only lead to unnecessary delay.

3. CALEA's compliance date (10/25/98) should be moved to enable sufficient time in which to install CALEA solutions in carriers' networks.

Estimates range between 18 and 30 months for the manufacturers need to convert technical standards into products and services ready for installation and deployment in carriers' networks. While CALEA allows carriers to request from the FCC extensions of this deadline, the FCC could be inundated with such requests from thousands of carriers, serving tens of thousands of facilities and services for which an extension would be required. Instead, since implementation has taken longer than anticipated when CALEA was drafted, and compliance by 1998 therefore is not reasonably achievable, the compliance date should be moved.

4. *Capacity requirements must be issued for carriers to be able to fulfill both their capacity and capability obligations.*

Capacity requirements must be consistent with historic electronic surveillance trends and must provide sufficient technical description to enable carriers and manufacturers to develop and install compliant hardware and software solutions.

*Conclusion:*

Telecommunications carriers look forward to continuing to work with law enforcement agencies in executing legally authorized electronic surveillance. While existing telecommunications facilities are providing electronic surveillance capabilities for law enforcement purposes, the industry recognizes its future responsibilities to design, develop and install surveillance capabilities as specified in CALEA. It is essential, however, in making the transition from present network facilities to future CALEA-compliant networks, that carriers are allowed to modernize their networks without CALEA coming back to haunt these carriers and their customers with potentially hundreds of millions of dollars of retrofitting expenses. By removing the clouds of uncertainty from the implementation of CALEA as recommended by USTA, CALEA can be implemented in a timely fashion.

Mr. McCOLLUM. Thank you, Mr. Neel, for describing what's down in the ditch.

Mr. Flanigan? We need to get the ox out, right? Mr. Flanigan, please proceed.

**STATEMENT OF MATTHEW F. FLANIGAN, PRESIDENT,  
TELECOMMUNICATIONS INDUSTRY ASSOCIATION**

Mr. FLANIGAN. Thank you, Mr. Chairman, for giving me the opportunity to appear before you and the other distinguished members of your committee. My appearance is on behalf of the Telecommunications Industry Association, TIA. TIA represents the manufacturers that supply the equipment that is the backbone of the telecommunications industry here in the United States and I'd like to add it's probably the finest in the country—the finest in the world.

My colleagues who are here representing the carriers: Mr. Neel, of course, for the wire line; Mr. Wheeler for cellular wireless; and Mr. Kitchen for the new PCS wireless—have all stressed the importance of the compliance dates. We fully support relief of these compliance dates.

My colleagues have already addressed several of the issues—that I had planned to discuss that is always a danger when you're the fourth one to talk. What I would like to do is address those issues that TIA is most intimately involved in, and they include 1) how the design and the manufacturing process works and why it takes so long, 2) the industry's effort to establish a CALEA standard

through the TIA standards process, and 3) where we are today in implementation of CALEA's capability and capacity requirements.

First, the design and manufacture process. We have a chart up there that reflects the average schedule for developing and deploying a CALEA standard. Although the development times vary from manufacturer to manufacturer, almost everybody that we have consulted says it requires at least 24 months to design and develop the CALEA standard. Then there's a deployment that's on top of that. What's involved here, as Mr. Wheeler had said earlier, is that there is a lot of code to be written. And as Mr. Neel mentioned, there are 26,000 switches out there in operation—each requiring many thousands of hours of code to be written by engineers.

This period of time (for developing the necessary software and hardware) is reflected in the chart in light blue. In addition, the same team of engineers must roll out this product, for one carrier and then another. The engineers have to do all the installation and get the bugs out of the new equipment. There is no small effort here in getting this deployment out.

Second, what CALEA intended and the industry's standards process is shown on another chart here. What we're showing is that CALEA provided a fairly logical process for implementation of both its capability and capacity requirements. First, the FBI was to promulgate its capacity regulation by October 25, 1995. About the same time, industry, in consultation with law enforcement, was to establish a capability standard. Industry would then have approximately 3 years to implement both the capacity and capability requirements, thereby meeting the October 25th, 1998 deadline.

To meet this time table, the industry began to work on the standard as soon as CALEA was passed. TIA, as the institution selected by industry to manage this process—set an ambitious schedule. We originally had planned a vote in early 1996 on the standard. We also actively invited law enforcement participation, hoping that this would help us arrive at a standard that was acceptable to all parties. Unfortunately, despite several concessions by industry, it gradually became apparent that law enforcement was insisting on the inclusion of more features than industry thought was required by CALEA.

In retrospect, we should have done what CALEA provides. We should have passed those features on which industry agreed as the safe harbor standard and then, if the FBI considered the standard to be deficient, it could have challenged this standard at the FCC. Instead, we continued to negotiate with law enforcement, trying to reach consensus at some acceptable middle ground. That's the process and that's what normally works. In the end, however, a compromise was not possible and industry decided to adopt only those parts of the standard on which industry and law enforcement were in agreement. At that point in early 1997, the FBI took several unfortunate actions which I believe current FBI management now regrets.

First, the FBI took the unprecedented step of seeking to have TIA's accreditation as an ANSI standards body revoked. This action was completely unwarranted. TIA's accreditation has never been challenged and we have had fifty years of history of developing standards. This challenge which the FBI eventually withdrew

lasted nearly 2 months and greatly polarized industry and law enforcement.

The FBI also decided to combine forces, as was mentioned earlier by Mr. Wheeler, the FBI, in a sense, stuffed the ballot box. Approximately 30 of the "no" votes received by TIA were identical using the same 74-page statement of opposition that the FBI had submitted.

So, where are we today? What can we do? As a result of the delay mentioned, industry finds itself only a year away from the October 25th, 1998 deadline with nothing to show but scars and legal expenses for 3 years of negotiations with law enforcement. Given the extensive lead times involved, even if a standard were announced tomorrow, manufacturers would not be able to deploy that standard until April 25th, in the year 2000. However, that is 10 months earlier than the anticipated capacity requirements which will not be in force assuming the FBI releases its requirements in January 1998, until January 2001.

In the past week, however, manufacturers have participated in a number of promising meetings with senior leadership at the Department of Justice and the FBI who have offered another opportunity to resolve the current impasse through good faith negotiations. Our concern about this proposal is that the next few months not resemble the last few years, with several meetings but no resolution of these tough issues. If that is so, we cannot afford to delay CALEA any longer. In our view it makes sense for industry to begin work on the 90 percent of the standard where there is already agreement, while at the same time trying to agree on the 10 percent that is in dispute. Otherwise, we are concerned that every day of discussions now could mean another day of potential delay.

In response to this concern, the officials, speaking for the highest levels of the Justice Department, have given us informal assurance that companies who begin in good faith to build at least the agreed part of the standard and promise to build any additional features that may be agreed upon later will not be threatened with sanctions on the October 25th, 1998 deadline.

We recognize that in return the Justice Department expects prompt efforts to reach agreement on the remaining 10 percent items, otherwise known as the "punch list." We are prepared to do this. We will explore this approach with the Department over the next several days, and we are hopeful that it will form the basis for a productive, new look at CALEA.

In conclusion, Mr. Chairman, manufacturers are pleased with the new signals we are receiving from the FBI. We have had more meetings with the FBI management in the past week, then we've had in the past several months. We believe that this is in substantial part because you were willing to hold this hearing and because the staff of the committee and subcommittee were willing to spend a considerable amount of time exploring the concerns of manufacturers before this hearing was held. For that, we thank you. And I'm happy to entertain any questions, Mr. Chairman.

[The prepared statement of Mr. Flanigan follows:]

PREPARED STATEMENT OF MATTHEW F. FLANIGAN, PRESIDENT,  
TELECOMMUNICATIONS INDUSTRY ASSOCIATION

A. INTRODUCTION

Thank you Mr. Chairman for giving me the opportunity to appear before you and the other distinguished members of your committee. No one can dispute that these hearings are timely and necessary. My appearance today is on behalf of the members of the Telecommunications Industry Association ("TIA"). TIA represents more than 600 United States companies that manufacture and supply the equipment that is the backbone of the telecommunications industry—from switches for landline, cellular, PCS and satellite systems to pagers to two-way radios.

Implementation of the Communications Assistance for Law Enforcement Act of 1994 ("CALEA") is at an impasse that industry and government have not been able to break. Congress intended that most of the implementation of the act would have occurred by the act's fourth anniversary, October 25, 1998. Regrettably, for the reasons I will discuss below, that deadline cannot be met.

I am pleased to report, however, that in the past week manufacturers have received a number of promising signals from the FBI. After several months of being excluded from meetings, last week TIA and several manufacturers were contacted by Mike Warren, the new section head for the CALEA Implementation Section at the FBI. He asked for a series of meetings and has offered to enter into good faith negotiations with the manufacturers, with the hope of achieving an agreement on CALEA's capability requirements.

Unfortunately, this is not the first time that such an appeal has been made by the FBI. In many ways, the FBI's current request is reminiscent of those we received when we first began the standards process in early 1995, immediately after the passage of CALEA.

At that time, the FBI approached TIA and asked, understandably, to be involved in the standards process. TIA was glad to welcome the FBI into the process, hoping that with the constructive participation of law enforcement we would be able to arrive at a standard that was acceptable to all parties. Indeed, as reflected in our Engineering Manual, TIA has always encouraged the active participation of government entities in our standards process.

Unfortunately, our attempts to avoid confrontation and at good faith negotiation with law enforcement have put us where we are today: a year away from the compliance deadline and still without a standard to which to build.

B. THE STANDARDS PROCESS

As the president of TIA, I am in a unique position to comment on the industry standards process and how we arrived at our current situation. TIA, as an institution accredited by the American National Standards Institute (ANSI), was selected by the telecommunications industry to promulgate the industry's CALEA standard.

Upon passage of CALEA, TIA promptly initiated a standards program. TIA set an ambitious schedule—hoping to complete the standard on an extremely expedited basis. Although there were some substantive disagreements within industry (as there always are in a standards process), these were resolved on a fairly rapid basis.

Disagreements with the FBI, however, were not so easily resolved. It gradually became apparent that law enforcement and industry had markedly different interpretations of what was required under CALEA.

In retrospect, we should have done what CALEA provides: passed the features on which industry agreed as the industry "safe harbor" standard and told the FBI that if it considered this standard to be deficient it should challenge the standard at the FCC. Instead, however, we accepted repeated FBI requests for more consultation, more meetings, and more drafts—all in the hopes of arriving at some acceptable middle ground where the FBI and industry could reach consensus.

In fact, for the past two and a half years, a vast majority of the standards meetings were devoted to addressing law enforcement's concerns and seeking such an agreement.

During these meetings, industry made several concessions to law enforcement, agreeing to include features in the standard that many in industry were convinced were not required under CALEA. For example, law enforcement requested that it be provided with continuous information about the location of an intercept subject's cellular phone, irrespective of whether the phone was being used or not. Industry refused to provide this feature, finding that it greatly exceeded what CALEA permitted. In a compromise, however, industry agreed to provide law enforcement with the location of a cell phone at the beginning and end of each call—even though

many industry participants felt that even this compromise exceeded the scope of CALEA.

As a result of such compromises, the current proposed industry standard (SP-3580) goes well beyond a conservative reading of CALEA and provides several of the additional features and capabilities requested by law enforcement during the arduous negotiations.

In the end, however, a consensus with the FBI could not be reached. The FBI insisted on at least eleven features (the "punchlist") that industry was convinced were not required even by the broadest reading of CALEA. TIA put these additional features to a vote in several standards meetings where they were broadly rejected by industry, for reasons that include lack of legal authority, cost, and privacy concerns.

Until that point, the negotiations (although protracted and often discordant) could at least be characterized as having been conducted in good faith. In early 1997, however, the FBI proceeded to take several unfortunate actions which I believe current FBI management now regrets. First, the FBI took the unprecedented step of seeking to have TIA's accreditation as an ANSI standards body revoked. This action was completely unwarranted. TIA's accreditation has never been challenged. If the FBI had been successful, TIA would have lost not just its ability to issue SP-3580 but its ability to issue any ANSI-related standards. This challenge, which the FBI eventually withdrew, lasted nearly two months and greatly polarized industry and law enforcement.

The FBI also decided to combine forces with state and local police departments to submit sufficient votes to defeat the industry's consensus proposal. Of the 65 ballots received on SP-3580, at least 34 were from state and local entities who previously had never participated in the standards process. Twenty-eight of these "no" votes were identical, using the same 74-page statement of opposition as the FBI submitted. (Only three companies filed negative comments and all three companies were only opposed to the compromise with law enforcement on location, considering the compromise to violate CALEA.) As a result, despite near-unanimous support among industry, adoption of a consensus standard was not possible.

In an effort to salvage something from this process, industry has decided not only to re-ballot the standard (although the vote on the re-ballot is unlikely to change) but also to place the standard on an alternative track that permits industry to privately consider whether the proposed standard should be adopted as a TIA "interim" (and ANSI "trial use") standard. Voting in this process will close on October 28. However, review and resolution of any comments on the ballots will not be completed until, at the earliest, mid-December. As a result, even if this "interim" standard is adopted, previous delays mean that industry will be unable to build to this standard in time to satisfy the October 25, 1998 deadline.

The purpose of retracing this history is not to criticize the FBI and certainly not to suggest that the current FBI leadership would act in a similar manner. It is necessary, however, to explain why we are here today. The FBI's assurances of good faith and offers to work out an accommodation are welcome, but we need to know that our past and future efforts to reach agreement with the FBI will not result in our being punished with lawsuits and fines in October 1998.

The compliance deadline for manufacturers is only a year away. Because of the extensive lead-times (24-36 months) required by manufacturers to design, build and deploy the equipment and software necessary to implement any complex standard, industry is already past the point of being able to comply with that deadline.

As a result, when the FBI asks us to enter into negotiations to resolve this problem we have to ask (and we think that it is fair for you to ask): What happens if, despite everyone's good faith effort, these negotiations fail to result in a compromise? Will the deadline now be four or six months closer while manufacturers still do not have a standard to which to build? Will manufacturers, despite their good faith efforts to negotiate a solution, be threatened with retroactive penalties of \$10,000 per day per wiretap order starting on October 25, 1998? Will the threat of such penalties be used to pressure manufacturers into building features that they do not believe are required by law?

These are questions that should be answered now. The industry shouldn't have to wait—they can't wait—for yet another round of negotiations with the FBI. Therefore, we ask for assurance, either from the Administration or from Congress, that manufacturers and carriers who participate in such good faith negotiations will be granted an extension sufficient to allow them to field CALEA-compliant equipment—and that this extension will not be conditioned on accepting the FBI's view of what CALEA requires.

### C. EXTENSION OF THE CAPABILITIES DEADLINE

The defeat of the safe harbor standard and the lack of any agreement on a uniform guideline for interception capabilities is the gravest issue facing the telecommunications industry. Without such a standard, manufacturers cannot fully commit to the extensive process of designing and deploying the equipment and software necessary to market products with uniform wiretap capabilities. As a result, it is virtually impossible, as of this date, for manufacturers to meet the rapidly approaching capability deadline of October 25, 1998.

Although development times vary from manufacturer to manufacturer, almost every manufacturer of telecommunications equipment operates on a research, design and implementation schedule that requires at least 24 months to make available new capabilities. In addition, manufacturers (working with their carriers) require several additional months (up to one year) to roll-out this new equipment. Even if a standard were announced tomorrow, under optimum conditions, manufacturers and carriers would have difficulty deploying the equipment to implement such a standard until, at the earliest, the spring of 2000.

Can manufacturers build CALEA-compliant equipment without a standard? We believe this would be foolhardy. The telecommunications industry is a standards-driven industry. Because of the great emphasis on interoperability, no manufacturer would dare begin designing a set of features as complex as CALEA requires without an industry standard. Not only would it be prohibitively expensive (requiring great engineering resources from each manufacturer), but it could also result in serious incompatibilities in various manufacturers' architectures.

An extension of the capabilities deadline is the only reasonable solution to the impending crisis. With an extension, industry and the FBI (perhaps with Congressional supervision) could undertake the serious negotiations proposed last week.

An extension of the October 1998 deadline would not increase the government's cost of reimbursing carriers. Nor would it severely affect law enforcement's current ability to conduct wiretaps. Because the FBI capacity regulations have not yet been promulgated, law enforcement will not have the capacity to conduct more than the number of cellular wiretaps they are already able to conduct until, at the earliest, November 2000.

For all of these reasons, Mr. Chairman, an extension is absolutely imperative. The October 25, 1998 deadline is not achievable. The window of opportunity has already closed.

### D. CAPACITY REQUIREMENT

As you are aware, the FBI has not yet promulgated its final capacity regulations. In part, the delay in announcing this standard was a contributing factor to the delay in the industry standards process. Throughout 1995 and early 1996, industry participants often postponed resolving certain issues pending the release of the capacity regulations and the equally anticipated Electronic Surveillance Interface. We understand from our recent discussions with the FBI, however, that the FBI intends to promulgate its standard this coming January. The industry certainly looks forward to the FBI regulations and appreciates the new leadership's efforts to resolve this matter.

However, even if a final regulation is promulgated in January, that capacity will not become available until January 2001. CALEA was drafted in an expectation that the capability and capacity requirements were to be implemented by the same October 25, 1998 deadline. Since capacity requirements will not be implemented until 2001, we see little point in trying to satisfy the capability on a considerably shorter implementation schedule—particularly because, without the capacity, law enforcement will be unable to conduct any more wiretaps they can currently conduct. It seems logical that industry should be given until the capacity deadline (whenever it is finalized) to provide CALEA's capability requirements.

### E. COST REIMBURSEMENT

Compliance with CALEA's capability and capacity requirements will be an enormous cost to manufacturers and carriers alike. Congress recognized this in CALEA and included provisions to reimburse carriers for the "direct costs" of developing modifications, capabilities and capacities as well as costs incurred in deploying such capacities and in training personnel. Despite this clear intent, the FBI promulgated rules that ignore this mandate. The regulations unnecessarily adopt complex accounting principles and methods applicable to federal procurement contracts that are unworkable for most manufacturers.

- The requirement to "flow down" cost accounting to manufacturers is beyond the FBI's statutory authority. The statute and its legislative history clearly indicate that telecommunications equipment manufacturers are to be paid by their carrier customers in the normal course of business based on commercial prices set by the marketplace.
- It is widely recognized that government contract-style cost accounting methods are costly and unnecessary when the government can obtain equivalent assurances that the costs being reimbursed by the government are reasonable. Alternatives such as a benchmark or reference pricing system would meet the government's needs.
- The FBI's argument that it must be granted unlimited rights in the design of the CALEA equipment and the data (software) provided with it are over-reaching and unworkable. A simple agreement between the lead carrier, the manufacturer and the government that the software development effort will be charged only once is all that is necessary.
- The regulations, without explanation or justification deny reimbursement to many categories of costs that Congress indicated should be reimbursed such as "general and administrative" ("G&A") costs.

Congress directed that the cost reimbursement regulations effectuate "cost efficient" payment for CALEA capabilities and capacity. These regulations are so regressive and complicated that they utterly fail to meet this requirement.

The Bureau has recently begun to explore new ways of pricing CALEA equipment. We are pleased that the FBI is now open to more commercially reasonable approaches. The FBI deserves encouragement from Congress for this effort. While many questions remain unanswered, we look forward to exploring this new approach in detail as the FBI develops its thinking further.

#### F. CELLULAR RELATED TECHNOLOGIES

Before concluding, Mr. Chairman, I would briefly like to talk about some technologies that have been largely ignored in the negotiations process. At the beginning of my comments, I mentioned the broad range of telecommunications equipment manufactured by TIA's member companies. Although the wireline, cellular and PCS industries are well represented here today and are the technologies most directly affected by CALEA, I should point out that TIA's member companies build equipment for several other related technologies, such as satellite telecommunications and paging, that also may fall within the scope of CALEA.

Individual companies have attempted to open dialogues with law enforcement about the status of these related technologies and how CALEA compliance should be managed. Unfortunately, law enforcement, in particular the FBI, has been so overwhelmed with the various issues related to cellular and PCS that they have been unable to talk about these other technologies.

Although we certainly appreciate their need to set priorities (as well as their informal statements that enforcement actions are unlikely for these technologies), as the October 25, 1998 deadline approaches for these technologies we need to receive some formal guidance from law enforcement (at a minimum, a formal assurance that the deadline will be extended).

#### G. CONCLUSION

In conclusion, Mr. Chairman, manufacturers are pleased with the new signals we are receiving from the FBI. We have had more meetings with FBI management in the past week than we had in the past four months. We believe that this is in substantial part because you were willing to hold this hearing and because the staff of the Committee and Subcommittee were willing to spend a substantial amount of time exploring the concerns of manufacturers before the hearing was held. For that, we thank you.

We are particularly pleased by the FBI's statement that it wishes to resolve the current impasse amicably through good faith negotiations. As I mentioned, however, we are in our current predicament because we have already devoted many months to efforts to reach a good faith understanding with the FBI, and all we have to show for it so far is a much-delayed standard. That's why we continue to ask for assurances that the FBI and Justice Department will not impose sanctions on carriers and manufacturers who have entered into such good faith negotiations and that they will give manufacturers sufficient time to comply with CALEA's capability requirements, whatever the outcome of those talks.

The FBI has presented several proposals aimed at putting CALEA implementation back on track, particularly regarding cost reimbursement and capability. Manu-

facturers, however, must judge the FBI by the flexibility it shows on the October 25, 1998 deadline.

All that manufacturers have ever wanted is a clear lawful standard to which to build and the assurance that we will have sufficient time to design and develop the necessary equipment and software to implement that standard. The proposals suggested by the FBI offer one of the most promising opportunities to resolving CALEA's implementation problems. But they do not solve the crisis that manufacturers have faced for the last eighteen months. I sincerely hope that the FBI can give us an assurance that this crisis can be defused. If not, then I believe only this Committee can provide the assurance that is needed.

Thank you, Mr. Chairman. I am would be willing to entertain any questions that you might have.

#### ATTACHMENTS

May 19, 1997 letter from Dave Yarbrough (Federal Bureau of Investigation) to Amy Marasco (American National Standards Institute)

June 19, 1997 letter from Dan Bart (Vice President, TIA) to Daisy Delogu (American National Standards Institute) with attachment [Note: the exhibits referred to in the attached statement are not included for sake of length; copies can be provided if requested]

July 3, 1997 letter from Edward Allen (Federal Bureau of Investigation) to Daisy Delogu

August 11, 1997 letter from Matthew J. Flanigan to Attorney General Janet Reno

September 9, 1997 letter from Matthew J. Flanigan to Attorney General Janet Reno

October 1, 1997 letter from Mike Warren (Federal Bureau of Investigation) to Matthew J. Flanigan

---

U.S. DEPARTMENT OF JUSTICE,  
FEDERAL BUREAU OF INVESTIGATION,  
TELECOMMUNICATIONS INDUSTRY LIAISON UNIT,  
Chantilly, VA, May 19, 1997.

Ms. AMY MARASCO, *Vice President and  
General Counsel, American National  
Standards Institute, New York, NY.*

DEAR Ms. MARASCO: I would first like to thank you, Ms. Daisy Delogu, and Ms. Ann Caldas for the assistance you have provided me during several telephone calls over the last few days.

As I mentioned in our discussions, I am very concerned about and disappointed in the recent actions taken by the Telecommunications Industry Association (TIA). Hence, I wish to appeal to ANSI's Executive Standards Council in regards to TIA's disregard of public comments related to *Standard Proposal (SP) 3580, Lawfully Authorized Electronic Surveillance* (ANSI BSR J-STD-25, EIA/TIA-715, and T1 LB-605). This standard was developed under the auspices of TIA and approved for a letter ballot on February 28, and, because TIA would like the document published as a new American National Standard, TIA provided the standard to ANSI for publication of the announcement for public comment in the *Standards Action*. ANSI has set a June 24 deadline for public comment.

This standard represents a cooperative effort by two of TIA's wireless standards formulating committees as well as a wireline subcommittee of Committee T1 sponsored by the Alliance for Telecommunications Industry Solutions (ATIS). Their goal was supposed to be the development of a standard which, when implemented, would enable law enforcement to intercept the call content and call-identifying information in light of advanced telephony including features such as call-forwarding, speed dialing, and call waiting. The impetus for the development of this standard stems from the passage of a federal law in October 1994, called the Communications Assistance for Law Enforcement Act, Public Law 103-414 (CALEA). CALEA clarifies the extent to which a telecommunications carrier must provide capabilities to assist law enforcement in conducting lawfully authorized electronic surveillance. In short, Section 107 of CALEA alludes to carriers and manufacturers availing themselves of "publicly available technical requirements or standards adopted by an industry association or standard-setting organization." Section 107(a)(2). Section 107 also provides that the Federal Communications Commission can establish by rule how the industry will provide this capability to law enforcement in the absence of such technical

requirements or standards. Section 107(b). The law also mandates the Attorney General, in coordination with local law enforcement, to consult with the telecommunications industry, including its standard-setting organizations, to "ensure the efficient and industry-wide implementation of the assistance capability requirements . . ." Section 107(a)(1). To that end, and under the authority granted by the Attorney General, the Telecommunications Industry Liaison Unit of the FBI, has been involved for several years in meeting and consulting with industry on this matter. In particular, representatives of TILU and other law enforcement agencies have regularly attended the meetings of the above-mentioned committees during the last twenty-four months while this standard was being developed.

It was during these meetings that law enforcement representatives were led to believe without any equivocation that the standard, when completed, would be issued as an ANSI standard as well as a TIA standard and, as such, the procedures which govern the approval process would be those developed by TIA to the extent that those rules do not contradict similar tenets set forth by ANSI in its written procedures. Also, if there were instances where the two sets of procedures were at variance, then the ANSI rules or policies would supersede those established by TIA. The question at hand involves the extremely important issue of whether the ANSI rules of due process and "openness" are being applied by TIA regarding public comment on SP-3580.

This problem first came to light last week when a letter by the U.S. Secret Service, providing comments on the standard, was rejected and return by TIA. I contacted Dan Bart, TIA's Vice President for Standards and Technology, on May 12 regarding this matter. He stated, essentially, that all comments must have attached or be associated with a particular ballot and that no comments would be accepted without a ballot. He stated that in the case of the Secret Service's letter, those comments would only be accepted by TIA if they were incorporated or attached to the federal ballot (which was to be submitted by TILU the following week). I asked Mr. Bart and he agreed that this means that if any individual wishes to comment on the standard, he or she must first pay \$136 (the price of the ballot) to obtain that right. Mr. Bart assured me that this was the procedure used for all TIA standards and that a similar fee was charged by ATIS as well.

My concern, which I believe is shared by the majority of law enforcement agencies that would like to provide comments regarding this standard, is that TIA's "no ballot-no comment" policy is fundamentally contrary to ANSI's policies of due process and openness. Section 1.2 of ANSI's *Procedures for the Development and Coordination of American National Standards* states that "any person (organization, company, government agency, individual, etc.) with a direct and material interest has a right to participate by: a) expressing a position and its basis, b) having that position considered, and c) appealing if adversely affected. Due process allows for equity and fair play" (emphasis added). Additionally, Section 1.2.1, titled "Openness," states that participation shall be open to all persons without financial barriers to participate nor shall their participation be conditional upon membership in any organization. Isn't "openness" stifled when a person must first pay \$136 to comment on what may become a public standard? Isn't "due process" violated when public comments are returned without any consideration of the matter or notice of appeal?

Due to the short time frame during which public comment will be received by TIA, and the fact that additional comments may be forthcoming from the law enforcement community as well as others, I am formally requesting that the Executive Standards Council convene and, if warranted (which clearly appears to be the case), expeditiously consider this matter and immediately intercede by compelling TIA to align its policy with ANSI's as it pertains to the acceptance and treatment of public comment of this standard.

In closing, I cannot too strongly emphasize the importance of developing a telecommunications standard which satisfies for law enforcement electronic surveillance requirements which are specified in CALEA. The U.S. Attorney General, the Director of the FBI, as well as prosecutors and law enforcement leadership across the United States and Canada are desirous that whatever standard is produced, is one that adequately provides for the capabilities that are required for the successful collection of evidence, the integrity of the intercept effort, and for the cost-effective management of interceptions. This standard is a beginning but is woefully deficient in several critical areas, and, I must add that TIA and most of its membership are aware of these facts. The telecommunications industry as a whole needs to be aware of law enforcement's formal comments on the balloted standard, whether or not those comments have a ballot attached. However, TIA is preventing these comments from being heard. Your intervention in this matter is critical and will send a signal that regardless of the outcome of the standard, the process by which it was devel-

oped and approved must embody the principles of due process, openness, and fair play as long as it bears the ANSI seal.

I would like to thank you in advance for your attention to this matter. We, as well as the law enforcement community who will be providing comments to TIA, eagerly await ANSI's efforts to quickly resolve this issue.

Sincerely,

DAVE YARBROUGH,  
*Supervisory Special Agent.*

TELECOMMUNICATIONS INDUSTRY ASSOCIATION,  
*Arlington, VA, June 19, 1997.*

DAISY DELOGU, *Program Manager,*  
*Procedures and Standards Administration,*  
*American National Standards Institute, New York, NY.*

Re: Your letter of May 28, 1997, concerning Appeal by Federal Bureau of Investigation to ANSI Executive Standards Council of TIA Procedures in the development of ANSI BSR J-STD-025, Lawfully Authorized Electronic Surveillance

DEAR MS. DELOGU: Your May 28, 1997 letter advised the Telecommunications Industry Association ("TIA") that Mr. Dave Yarbrough, Supervisory Special Agent of the Federal Bureau of Investigation ("FBI"), has "formally appealed to the Executive Standards Council ("ExSC") the procedures being followed by TIA in the development of ANSI BSR J-STD-25, Lawfully Authorized Electronic Surveillance." You attached to your letter a May 19, 1997 letter from Mr. Yarbrough to Amy Marasco, Vice President and General Counsel of ANSI, setting forth the FBI's specific concerns. You asked for a responsive statement from TIA on or before June 18, 1997, and further advised that a hearing will be held at ANSI Headquarters in New York to assist the ExSC in their evaluation of this situation. You indicated the hearing may occur in July and that TIA and Mr. Yarbrough will be invited to attend the hearing.

Fran Schrotter of ANSI granted a TIA request to extend the reply date to June 20, 1997 since most ANSI staff concerned with this matter were at an ExSC meeting and would not be in New York to receive the response and since most TIA staff were unavailable during the first week of June due to SUPERCOMM97 and thus could not work on the response. Also, the TIA President considers this a serious matter and wants to review the response and he will not be returning to the office until June 19, 1997 from the International Telecommunication Union's ("ITU") ASIA Telecom show in Singapore.

Attached to this letter is the "Responsive Statement of TIA to the Appeal of the Federal Bureau of Investigation to the Executive Standards Council of the American National Standards Institute regarding TIA procedures used in the development of ANSI BSR-J-STD-025, Lawfully Authorized Electronic Surveillance, a proposed Joint American National Standard of TIA and Accredited Standards Committee T1." As indicated in the detailed response, many of the factual statements in Mr. Yarbrough's letter are not accurate. The response also raises some collateral issues as to whether the FBI is trying to delay the issuance of this standard.

I am sending the main response by Email and Facsimile and will overnight the attachments to you and others. Please provide me the date for the Hearing if you determine one is required, a rough idea of the amount of time the Hearing is likely to take, a copy of any procedures to be followed at the ExSC Hearing, whether TIA can be represented or accompanied by counsel at the Hearing, whether witnesses are permitted, and whether other interested parties can observe the proceeding or provide input.

Should you or Amy Marasco or the Chair of the ExSC have any questions on the attached, please do not hesitate to contact me.

Sincerely,

DAN BART, *Vice President,*  
*Standards and Technology.*

cc A. Marasco, ANSI General Counsel  
A. Caldas, ANSI Staff  
G. Ziegenfuss, Chair, ExSC  
D. Yarbrough, FBI  
S. Miller, Alliance for Telecommunications Industry Solutions  
G. Peterson, Chair, Committee T1  
P. Vishny, TIA Counsel  
L. Petak, FCC

K. Tran, Secret Service  
J. Pignataro, FBI TILU, State and Local Law Enforcement

Attachments

---

RESPONSIVE STATEMENT OF TIA  
JUNE 19, 1997

DAN BART, VICE PRESIDENT, STANDARDS AND TECHNOLOGY TELECOMMUNICATIONS  
INDUSTRY ASSOCIATION

*Introduction to TIA*

TIA is a full-service trade association of over 600 U.S. companies which manufacture and/or supply communications and information technology equipment, products, systems, distribution services, and professional services throughout the world. TIA's members collectively provide the bulk of the physical plant and associated equipment and software used to support and improve the nation's telecommunications infrastructure and the infrastructures of many other countries around the world. TIA represents the telecommunications sector of the overall electronics industry in association with the Electronic Industries Association ("EIA"). For more information on TIA, Exhibit A is a copy of TIA's 1996 Annual Report.

In addition to its trade association role, TIA is also a Standards Development Organization ("SDO") which creates standards and other technical documents and is organizationally accredited by the American National Standards Institute ("ANSI") to develop American National Standards. In that capacity, TIA's product-oriented divisions sponsor Engineering Committees and Subcommittees which are open to parties who have a direct and material interest in the technical work within the respective jurisdiction of the TIA Formulating Groups. TIA membership is not a prerequisite to participation. TIA and its predecessor organizations have been actively involved in developing standards for the industry for over 50 years. Further information concerning TIA, its standards program, and the agreement pursuant to which ANSI BSR-J-STD-025 Lawfully Authorized Electronic Surveillance, has been developed together with ANSI Accredited Standards Committee T1, is set forth in the extensive discussion which follows:

*Specific Reply to the Allegations of Mr. Yarbrough in his Letter of May 19, 1997*

Mr. Yarbrough, in his letter of May 19, 1997, makes the following allegations which are within the jurisdiction of the ExSC concerning TIA's actions:

1. That TIA has disregarded public comments related to Standards Proposal 3580;
2. That TIA has violated the ANSI rules of due process and "openness" regarding public comment in connection with the aforesaid Standards Proposal because it rejected and returned comments and because it required the payment of the price of the draft standard to submit comments.

These allegations are simply erroneous.

Mr. Yarbrough also made some other minor factual misstatements and discussed some issues regarding the technical content of the document which are not matters within the jurisdiction of the ExSC but, for the sake of completeness, TIA will provide substantial information on these matters also since this information may provide insight as to why this Appeal was filed at all.

It is not true that TIA "rejected and returned" a letter by the U.S. Secret Service which provided comments on the proposed standard. In fact, the letter in question was included in the ballot summary for the Formulating Group and copies were provided to the group which is charged with the task of considering the letter's appropriateness and relevance to the matter being balloted.

Nor is it correct to say that, in order for an individual to submit ballot comments, the individual must first pay \$136.00 as the price of a ballot. Perhaps the procedures of TIA were not understood by the person making the inquiry. In the proceeding involved, the FBI made a filing on behalf of the Federal Government and a suggestion was made to the U.S. Secret Service that it associate its comments with the FBI ballot and filing. However, comments received by an interested party, with a ballot, and without the payment of any fee, would also be accepted. The charge of \$136.00 was nothing more than the sales price for copies of the draft standard BSR-J-STD-025 (SP-3580). This single copy price was also indicated in the *Standards Action* notice of April 25, 1997 published by ANSI. It is, of course, the expectation that parties submitting comments will be familiar with the document on which they are making the comments. If parties are able to review the document without pur-

chasing it, the ballot and comment would nonetheless be accepted. Thus, as can be seen, participation in the public comment stage is *in fact* afforded by TIA to all persons without financial barriers and without being conditioned upon membership in TIA or any other organization.

While TIA believes that this explanation should be sufficient to dispose of the Appeal in question, TIA wishes to call to the attention of the Executive Standards Council the fact that the subject matter of the standard involved reflects serious disagreements between the United States telecommunications industry on the one hand, and law enforcement agencies ("LEA") on the other hand. Consequently, TIA is taking the liberty of providing the Executive Standards Council with the following additional extensive information concerning this matter.

#### *TIA Standards Program*

Prior to 1988, TIA's standards program was a part of the EIA Information and Telecommunications Technology Group ("EIA ITG"). With the merger of EIA ITG and the United States Telecommunications Suppliers Association which was then re-named TIA, responsibility for what were EIA telecommunications sector standards belonged to TIA. From 1988 to January 1992, these EIA/TIA standards were developed in accordance with the EIA ANSI-accredited process. In January 1992, TIA became separately ANSI-accredited based on its December 1991 Engineering Manual and standards generated under that process are typically designated by the prefix TIA/EIA. The Formulating Group determines the type of document it wishes to develop under the ANSI-accredited TIA Engineering Manual, up to and including American National Standards ("ANS"). From time to time, the TIA Engineering Manual is interpreted and occasionally supplemented by Advisory Notes issued by the TIA Standards and Technology Department. Any changes to the Engineering Manual must first go through an internal TIA balloting procedure and then be forwarded to ANSI for approval. For example, TIA recently expanded eligibility for voting participation in its Formulating Groups beyond U.S. organizations to include Canadian and Mexican organizations and that change is pending at ANSI. For additional information on the TIA standards program and for use in this Appeal, TIA has attached the following: *Exhibits B, C, and D*, copies of TIA Standards and Technology Annual Reports ("STAR") for 1994, 1995, and 1996; *Exhibit E*, a copy of the TIA 1991 Engineering Manual; and *Exhibit F* a copy of all current TIA Advisory Notes.

From time to time TIA works with other SDOs both here and abroad to share information, collaborate on technical work, and sometimes to use each other's standards or to issue joint standards. This has included such organizations as the International Telecommunication Union ("ITU"), Canadian Standards Association ("CSA"), the European Telecommunications Standards Institute ("ETSI"), Telecommunications Technology Association of Korea ("TTA"), Telecommunications Technology Committee of Japan ("TTC"), Australian Telecommunications Standards Committee ("ATSC"), ANSI Accredited Standards Committee T1, and others.

TIA has an agreement with Committee T1 to issue Joint Standards Documents ("JSD") in selected areas where both SDOs have an interest in and something to contribute to the work. This Appeal concerns such a proposed JSD. *Exhibit G* is a copy of the TIA/T1 JSD Agreement. Under the JSD Agreement, either TIA or Committee T1 is given the lead on a particular proposed standard and then the procedures of that lead SDO govern the detailed development process and the non-lead organization is considered an "interested party" in the work and the Secretariat is provided copies of all ballots for distribution to that SDO's membership. Voting rights are determined however by the lead organization's procedural manual. TIA's TR-45.2 is the lead on ANSI BSR J-STD-025.

#### *Background on CALEA and SP-3580*

In 1994 Congress passed and the President signed into law the Communications Assistance for Law Enforcement Act of 1994 ("CALEA"), Pub. L. 103-414. This law addressed various concerns raised by law enforcement that advancements in digital telephony were eroding Law Enforcement Agencies ("LEA") ability to conduct court-authorized electronic surveillance or "wiretapping." The legislation was intended to preserve the status quo in terms of government surveillance and without expanding government capabilities. Congress stressed that the requirements of CALEA should be narrowly interpreted. The telecommunications industry, both manufacturers and service providers, have had a long history of cooperation with LEA to effect court authorized electronic surveillance.

CALEA provides a "safe harbor" from enforcement for service providers and manufacturers who install or retrofit equipment that meets the requirements of "publicly available" industry standards "adopted by an industry association or standard-

setting organization." (CALEA, Section 107) Sections 103 and 107 of CALEA allow for multiple industry or even individual carrier technical solutions to implement law enforcement requirements. The FBI is expressly prohibited (Section 103) from dictating or requiring system design features. For use by ANSI and ExSC, *Exhibit H* is a copy of a Cellular Telecommunications Industry Association ("CTIA") booklet containing a copy of CALEA and summary of its requirements for the wireless industry.

The House Report on H.R. 4922, Rept. 103-627, which became CALEA states (pp. 26-27):

Section 2606 establishes a mechanism for implementation of the capability requirements that defers, in the first instance, to industry standards organizations. Subsection (a) directs the Attorney General and other law enforcement agencies to consult with associations and standards-setting bodies of the telecommunications industry. Carriers, manufacturers and support service providers will have a "safe harbor" and be considered in compliance with the capability requirements if they comply with publicly available technical requirements or standards designed in good faith to implement the assistance requirements.

. . . The use of standards to implement legislative requirements is, of course, appropriate so long as Congress delineates the policy that the guidelines must meet (citations omitted). . . . The authority to issue standards to implement legislation delegated here to private parties is well within what has been upheld in numerous precedents. (citations omitted)

. . . The appropriateness of the delegation here is furthered by two factors: (1) Compliance with the industry standards is voluntary, not compulsory. Carriers can adopt other solutions for complying with the capability requirements; and (2) The FCC retains control over the standards. Under section 2602(b), any carrier, any law enforcement agency or any interested party can petition the FCC, which has the authority to reject the standards developed by industry and substitute its own.

Thus, Congress provided a mechanism that deferred in the first instance to CALEA implementation by industry, with consultation with but not control by the FBI, and an oversight mechanism in the Federal Communications Commission (FCC).

Industry has three incentives to comply with CALEA and to develop appropriate industry standards to implement CALEA: (1) A safe harbor from the punitive enforcement provisions of the law by compliance with the industry standard; (2) A desire to fully meet CALEA capability requirements lest the FCC determine the standard is deficient under CALEA; and (3) A reimbursement program for retrofitting equipment to meet CALEA requirements when paid for by LEA.

The FBI however has incentives to delay the industry standards process since (1) LEA want "more" than the minimum CALEA technical capabilities covered in the proposed standard since this will make their jobs easier even if such expanded capabilities for electronic surveillance go beyond the status quo envisioned by Congress when CALEA was enacted; (2) Any features beyond the "floor" of CALEA may end up funded at the carrier's expense since reimbursement is limited to requirements to implement CALEA; and (3) Failure to adopt an industry standard and the safe harbor it provides will allow the FBI to use the threat of punitive enforcement actions to extract concessions from manufacturers and carriers for features beyond CALEA.

The tension created by industry's desire to fully meet but not exceed CALEA capability requirements versus LEA's and the FBI's efforts to delay the process and expand the features encompassed within the proposed standard has generated front page stories in the New York Times, extensive coverage in the trade press, massive lobbying efforts by the LEA within the industry and on Capital Hill, and this Appeal.

Various organizations, both industry associations and organizations representing privacy advocates, have found it necessary to rebut FBI statements made to Congress regarding CALEA implementation. *Exhibits I* contains a response from TIA to the FBI's CALEA Implementation Plan filed with various Committees of the House and Senate; *Exhibit J* is a response sent to the same House and Senate Committees by CTIA, the United States Telephone Association ("USTA"), the Personal Communications Industry Association ("PCIA"), and the Center for Democracy and Technology ("CDT"); and *Exhibit K* is an Interim Report on "Communications Privacy in the Digital Age" (June 1997), issued by CTIA, CDT, USTA, Center for National Security Studies, Commercial Internet eXchange Association, Competitive Telecommunications Association, and the Electronic Messaging Association. This Interim Report was prepared by the Electronic Surveillance Task Force of the Digital

Privacy and Security Working Group ("DSPWG") and contains a lot of background on the current issues surrounding CALEA Implementation and other privacy topics. TIA is a member of DSPWG.

In addition to its domestic efforts to advocate expanded surveillance capabilities, the FBI has also met with other countries' LEA and developed an international agenda to try to persuade the ITU to undertake international harmonization of technical requirements for legal interceptions of telecommunications. *Exhibit L* is a May 21, 1997, letter (two days after the letter to ANSI for this Appeal) from the FBI to the Department of State urging the State Department to have the ITU consider technical capabilities for interception of telecommunications even before there is an agreed upon U.S. standard. At a State Department meeting on June 11, 1997, with broad private sector and public sector participation, this FBI position was determined to be premature until a U.S. consensus position is finalized. Thus, while trying to *slow down* the U.S. process for a standard which complies with CALEA but does not have FBI-desired expanded capabilities, the FBI is trying to *make haste* internationally.

The FBI's Telecommunications Industry Liaison Unit ("TILU") and LEA personnel who work with TILU have also written letters to senior level executive personnel at trade associations, manufacturers, and service providers, claiming the proposed standard is "deficient," misstating that TIA "rejected" some comments from the Secret Service, lobbying them to expand the standard to include "missing capabilities," and wanting "assurances" that the FBI's point of view will be included in the final standard even if such expanded capabilities are beyond what CALEA intended. *Exhibits M and N* are copies of letters sent to TIA's President by a TILU participant, and TIA has been advised that Presidents and Chief Executive Officers of carriers and manufacturers have received similar letters.

TIA believes that ANSI staff and the ExSC must have an understanding of all the industry and CALEA background issues so that they can place the subject Appeal in the context of other FBI initiatives with respect to expanded surveillance capabilities beyond those required by CALEA, since such data may provide an insight as to why this Appeal, based on an erroneous statement of facts, was initiated.

TIA's Subcommittee TR 45.2 began work analyzing CALEA shortly after it was signed into law in October 1994. By early 1995 there had been considerable discussion among industry participants about the need for Congressionally contemplated "industry standards" for CALEA. A Project Number ("PN") 3580 was assigned for the new work "to create baseline text for inclusion in appropriate standards projects." The standard would focus on technical "capabilities" for lawfully authorized electronic surveillance while TILU and the Department of Justice ("DOJ") worked on "capacities" for interceptions, a figure driven by geographic crime rates and past experience. Congress had contemplated that the final capacity requirements would be issued within a year of enactment of CALEA, and if not, then the capacity requirements would need to be met 3 years after a final capacity notice—now no sooner than the year 2000 since the FBI has delayed issuing the final capacity notice. Under the current law, "capability" requirements would need to be available—presumably for a single interception—no later than October 1998 unless that date were extended by the FCC or Congressional action.

Work progressed in TR 45.2 for a CALEA-compliant standard and the draft document, known then as PN-3580, was taking shape. In the meantime, the FBI contracted with a consultant to develop what is generally known as the Electronic Surveillance Interface ("ESI") which was and is a "wish list" of capabilities that LEA would like to have for electronic surveillance, including unrealistic timing constraints, a "tracking" beacon use of wireless telephones, etc. Eventually the FBI made the ESI a contribution to the Formulating Group. This caused a delay in the work as the ESI was then compared to the capabilities contained in the PN-3580 draft. Where no justification could be found in CALEA for the capability—even though conceding such capability might be helpful to LEA—the Formulating Group revised the text to ensure that the proposed standard used CALEA as a floor and a ceiling.

The issue was not whether a capability was technically possible, but whether it is required by CALEA. For example, CALEA does not require location information of the calling or called party, but if it is available in the system, then it can be provided for in the court order, but not as a CALEA mandate. This is an important distinction since CALEA has requirements for retrofitting of existing systems under certain circumstances. However, the reimbursement is for only CALEA requirements. An additional consideration was that if capabilities beyond CALEA were included in the standard, this would make the implementation more complex thus risking delays in the statutory compliance dates and further running the risk of costs for those features not being allowed as a CALEA compliance expense. Industry

offered to generate a separate document containing all the expanded and non-CALEA capabilities that the FBI could separately fund with a service provider, but this was refused by the FBI which chose to try to get everything LEA wanted—whether required by CALEA or not—into the draft standard.

When the debate turned too “legalistic” for the engineers in the Formulating Group, the CTIA hosted Legal Summit meetings to allow all parties to air their views and then attorneys for particular organizations could direct their standards participants how to vote on specific text for the draft document at the next Formulating Group meeting. Along the way it was decided to have one document for wireline and wireless and to produce a Joint Standards Document (“JSD”) with Committee T1. There was discussion about whether it should be an ANS and TR 45.2 voted to issue the ballot as a proposed American National Standard in order to seek the widest range of inputs on the document and its compliance with the mandates of CALEA, including non-traditional standards participants such as privacy advocates and others.

Standards Proposal (“SP”)–3580 was issued in March 1997. Copies were widely distributed in TIA and to other TIA Formulating Groups that had an interest in the work. Per the JSD agreement copies were provided to the Alliance for Telecommunications Industry Solutions (“ATIS”) the T1 Secretariat for Letter Ballot in T1. TIA sent copies to other SDOs like ETSI where we exchange each other’s draft standards. TIA generated a Press Release announcing the availability of SP–3580, listed SP–3580 in TIA’s *Industry Pulse*, posted notice on TIA’s Web Page, and provided a BSR–8 to ANSI for ANSI *Standards Action* notice.

ANSI gave notice of BSR J–STD–025 in the April 25, 1997 issue of *Standards Action*, page 7, attached as *Exhibit 0*. TR–45.2 had a closing date of May 12, 1997 to get ballot responses and comments. (Due to clerical error, the copies of SP–3580 did not indicate that this would be a JSD or indicate the J–STD–025 number, if approved, but this was corrected in time for the ANSI notice, and Formulating Group members informed.) T1 issued a Letter Ballot (LB–605) with a closing date of May 9, 1997 in order to meet the TR 45.2 date. An initial meeting to start Ballot Comment resolution was held May 20, 1997, in Washington, DC, and Ballots and Comments are still open due to the ANSI Public Inquiry close date of June 24, 1997. TIA has been advised that other trade associations also advised their members of the public inquiry on this important proposed standard. TIA was also advised that the FBI notified various LEA of the public balloting of SP–3580. There has been trade press and other coverage of the balloting. TIA is not aware of any TIA or other SDO standard that has had this degree of notice and “openness” and call for public comment.

In accordance with paragraph 6.4 of TIA’s ANSI-approved Engineering Manual: “Copies of Standards Proposals shall also be available upon request from TIA during the comment period. An appropriate fee, not to exceed the anticipated sales price of the finished standard, may be charged for Standards Proposal copies.” EIA’s Publication Department which handles TIA’s distribution to our publisher, Global Engineering Documents, determined that the anticipated sales price of the finished standard would be around \$136.00 and this single copy price, was indicated in the *Standards Action* notice of April 25, 1997. Parties were advised by ANSI to order the draft standard BSR–J–STD–025 (SP–3580) from Global Engineering and to send Ballot/Comments to TIA’s Secretariat with a copy to ANSI’s Board of Standards Review (“BSR”). The Ballot Form is included with the draft standard.

In addition, at the written request of the FBI, TIA granted a royalty-free copyright license for forty (40) copies of SP–3580 for internal distribution of SP–3580 at the FBI. TIA also discussed with the FBI bulk pricing if it desired to purchase bulk copies of the draft standard, as well as a royalty-bearing copyright license to distribute “informational only” copies to various state and local LEA. The FBI never formally requested or received bulk pricing or any other further copyright licenses to the draft standard.

#### FURTHER COMMENTS ON THE MAY 19, 1997 FBI LETTER

As of the date Mr. Yarbrough had written his letter, and to this date, TIA has not “disregarded” any public comments related to SP–3580 or ANSI BSR J–STD–025. Ballots with Comments are still coming in and they are being copied by the TIA Standards Secretariat and forwarded to the Formulating Group. The balloting window is open until June 24, 1997. As part of the ANSI-approved process each will be looked at for appropriate action or response under the TIA Engineering Manual.

The proposed standard represents more than cooperation with just two of TIA’s Formulating Groups, one T1 subcommittee, and law enforcement as stated by Mr. Yarbrough. TR–45, Mobile and Personal Communications, and TR–46, Mobile and

Personal Communications Systems were involved, as well as T1P1, T1S1, and there were liaisons with TR-34 and TR-41. With regard to "openness" or "due process," the FBI is incorrect that TIA "rejected" and "returned" a U.S. Secret Service letter. In point of fact, the letter was included among all comments and ballots copied by the TIA Standards Secretariat and given to the Chair of the Formulating Group. *Exhibit P* is the first Ballot summary provided to the Chair and the U.S. Secret Service letter is listed and copies were provided to the Formulating Group.

What did occur was a call to the U.S. Secret Service asking whether they wanted to approach the FBI and have the Secret Service comments included with the Ballot Form that TIA understood the FBI was casting on behalf of the U.S. Federal Government. To the extent that one federal agency's input might be at odds with the lead agency's comments, TIA assumed the Federal Government would like to resolve such issues internally in order to have a singular response on the Federal Government Ballot. TIA's ANSI-approved Engineering Manual provides one company one vote and one vote for the Federal Government.

In my conversation with Mr. Yarbrough, I did advise that TIA charges a fee for draft standards as allowed by our ANSI-approved Manual and that the Ballot Form is included with the copyrighted draft standard. I explained to him that TIA's Engineering Manual has two demonstrations of consensus, one within the Formulating Group to issue the Standards Proposal for a TIA standard and an American National Standard, and another consensus demonstration as a result of the public ballot. (See section 6.4 of TIA Engineering Manual). Since a mere comment letter could be in support of a Yes vote or in support of a No vote, the TIA Manual requires a Ballot Form so that there is no doubt of how an interested party is voting on the proposed standard.

TIA believes its process as documented in the ANSI-approved TIA Engineering Manual is open, has guarantees of due process, and provides for a right of Appeal internal to TIA and in some cases to ANSI as well. "Publicly available standard" does not equate with "free" standard. Given the enormous costs of *running*—and in these days of competitive standards setting and to deal with other issues legally *defending*—a standards development program, a modest fee of \$136.00 to purchase a draft standard and help contribute to cost recovery of expenses is not a bar to openness. Given FBI statements about what an important "weapon" electronic surveillance is in the war on crime, TIA notes that the cost of the draft standard is approximately 1/3 the cost of a Smith and Wesson 38-caliber pistol based on a recent telephone inquiry—another popular weapon used in the war on crime by LEA. TIA also notes that Congress authorized \$500 million for CALEA implementation and \$136.00 is *de minimus* when compared to this funding level.

TIA does not condition participation in its Formulating Groups by membership in any organization. Since TIA members pay dues to TIA to help sponsor the costs, that is one revenue stream. Organizations who are not TIA members are required to pay a non-TIA-member fee to help contribute to cost recovery since they are not TIA dues payers.

Contrary to the FBI's allegations of lack of openness for LEA comments, TIA's Manual expressly *waives* this non-member fee for government participation in Formulating Groups on a *non-voting* basis. Copies of all Notices, Agendas, Contributions, Hotel Meeting Expenses, etc., are provided without any financial support from such government participation. However, to have *voting* rights in the Formulating Group, the non-member fee would be required. (See Section 3.2.4) Thus, the FBI and other law enforcement personnel on the TR-45.2 mailing list who participate in the standards work received *free* copies of the draft standard as did the industry members who supported by dues or non-member fees such work. For the ANSI public inquiry, unlike the vote at the Formulating Group level, the FBI *did* have voting rights without the payment of any fee since it is TIA's practice to afford *any* directly and materially interested party, as referenced in the TIA Engineering Manual, voting privileges at the time of the public inquiry phase. TIA requires a showing of consensus in the Formulating Group and in the public inquiry phase for a TIA standard that is an American National Standard. There is a one company one vote rule and the Federal Government gets one vote, however. This is more openness than ANSI procedures require and more openness than most other SDOs that TIA coordinates with. Although there is a charge for the draft standard, there is no direct fee to cast the ballot.

As mentioned, no public comments have been returned by TIA to any party. If Negative Ballots remain at the end of the consensus process, those parties will be advised of their right to Appeal. Such rights are clearly specified in the Manual, Annex A, Section A5. To TIA's credit, since 1988, when TIA was created, there has only been one formal Appeal taken under this Annex all the way to a TIA Appeals Panel. That Appeal did not involve an American National Standard.

TIA's members and other industry participants in the TR-45.2 work on this draft standard believe the proposed text "satisfies for law enforcement electronic surveillance requirements which are specified in CALEA." Whether the proposed standard goes beyond CALEA and satisfies every wish list item desired by law enforcement is a different question and not the end point sought by this particular Standards Proposal. Under the statute, the standard is deficient only if it does not meet the CALEA requirements. The content of the standard is not a matter for ANSI or the ExSC, and whether or not the standard is deficient in meeting CALEA is within the sole jurisdiction of the FCC.

CONCLUSION

TIA respectfully asserts that its procedures in the development of the proposed American National Standard satisfy ANSI's requirements as specified in our accreditation file. Thus, this Appeal should be dismissed.

U.S. DEPARTMENT OF JUSTICE,  
FEDERAL BUREAU OF INVESTIGATION,  
Washington, DC, July 3, 1997.

Ms. DAISY DELOGU, *Program Manager,*  
*Procedures and Standards Administration,*  
*ANSI, New York, NY.*

DEAR MS. DELOGU: This will confirm our telephone conversation on July 1, 1997 in which I advised you of the FBI's desire to withdraw out appeal to the Executive Standards Council for a review of procedures being followed by the Telecommunications Industry Association (TIA) in the development ANSI BSR J-STD 25. I have discussed this matter with Mr. David Yarbrough, FBI, and Mr. Dan Bart, Vice President of Standards and Technology, TIA. I am confident of TIA's commitment to the fair and equitable application of TIA's and ANSI's procedures during the development of this standard. We have agreed that continued discussions between TIA and law enforcement will ensure a better understanding of each party's concerns.

Thank you for your interest and assistance in this matter.

Sincerely,

EDWARD L. ALLEN, *Chief,*  
*Electronic Surveillance*  
*Technology Section,*  
*Information Resources Division.*

TELECOMMUNICATIONS INDUSTRY ASSOCIATION,  
Arlington, VA, August 11, 1997.

Hon. JANET RENO, *Attorney General,*  
*U.S. Department of Justice,*  
*Washington, DC.*

DEAR MS. RENO: The Telecommunications Industry Association (TIA) has learned that a meeting concerning the current deadlock between the Federal Bureau of Investigation and the telecommunications industry with respect to implementation of CALEA was scheduled for telecommunications carriers and their associations at your offices on August 12, 1997. TIA understands that the meeting has now been canceled, however, we ask to be considered for participation in any future meetings regarding CALEA.

TIA is a full-service trade association of more than 600 members who manufacture and supply communications and information technology equipment and service throughout the United States and abroad. TIA represents both large and small companies which collectively provide the bulk of the physical plant and associated equipment for the industry. In addition, TIA is accredited by the American National Standards Institute (ANSI) to issue American National Standards for the industry. TIA also testified before Congress on the CALEA legislation.

While TIA is encouraged that the Department of Justice has decided to become actively involved in the resolution of CALEA issues, our members are perplexed that you would not involve in these important discussions the manufacturers of the equipment that must be modified. Congress specifically provided a role for manufacturers in CALEA, see CALEA section 106. TIA is also the lead organization establishing the industry standard for CALEA as contemplated by section 107. Discussing these significant issues with carriers only is similar to the government calling together automobile dealers and their associations to discuss government require-

ments for new safety designs to cars, but not inviting the big three auto manufacturers.

We do not believe much progress can be made with respect to deciding which of the wiretap capabilities requested by the FBI can be accomplished unless the companies who need to conceive, design and implement these changes are present. While the carriers are likely to know what it is they are inclined to buy, only the manufacturers can definitively opine on what can be made and in what time frame the equipment can be developed and distributed to service providers. CALEA puts significant requirements on both carriers *and* manufacturers. Without both considering the issues, a solution will not be found.

Although there are hundreds of carriers, there are only a handful of manufacturers that make up the majority of the market in telecommunications equipment. Accordingly including the primary manufacturers and their trade association would only increase the size of the meeting by a few seats. TIA would be pleased to coordinate with your office to identify the representatives of the primary telecommunications equipment manufacturers.

Please feel free to call me or Grant Seiffert, Director of Government Relations of my staff, for additional information at (202) 383-1483. Thank you for your attention to this important matter. TIA believes that future participation would enable manufacturers to explain their concerns and to provide any necessary CALEA background in greater detail that will benefit all interested parties.

Sincerely,

MATTHEW J. FLANIGAN, *President.*

---

TELECOMMUNICATIONS INDUSTRY ASSOCIATION,  
Arlington, VA, September 9, 1997.

Hon. JANET RENO, *Attorney General,*  
*U.S. Department of Justice,*  
*Washington, DC.*

DEAR MS. RENO: The Telecommunications Industry Association (TIA) has learned that the Department has conducted negotiation meetings with telecommunications carriers concerning the implementation of CALEA, but has, again, decided not to invite the companies that manufacture the telecommunications equipment that is the subject of these negotiations. The most recent negotiations conducted at the Department, *inter alia*, attempted to convince the carriers to purchase certain telecommunications features that law enforcement considers to be important, but which are not required by law.

Implementation of the features sought by the government is a matter that requires manufacturer participation. The complexity of implementing such features is likely to vary significantly from manufacturer to manufacturer and from platform to platform. While eventual agreement by carriers that they would be willing to introduce desired wiretap capabilities might be necessary, this ignores the critical question of whether such features are achievable and on what time schedule they might be created. Carriers cannot possibly address that question. We urge the Department to consider whether concessions from carriers alone would have any meaning or reasonable prospect of solving the significant technical and legal problems precluding full implementation of CALEA and whether carrier-exclusive discussions are a productive use of time and resources.

TIA stands ready to coordinate the participation of telecommunications manufacturers in future discussions with the Department. Grant Seiffert, Director of Government Relations, would be pleased to coordinate this issue with your staff.

Sincerely,

MATTHEW J. FLANIGAN, *President.*

cc: Steven Colgate, AAG  
Robert S. Litt, DAAG  
Congressman Harold Rogers  
Senator Judd Gregg

---

U.S. DEPARTMENT OF JUSTICE,  
FEDERAL BUREAU OF INVESTIGATION,  
Washington, DC, October 1, 1997.

Mr. MATTHEW J. FLANIGAN,  
Arlington, VA.

DEAR MR. FLANIGAN: On behalf of the Attorney General and the Director of the FBI, I am writing to you in response to your letter to the Attorney General dated 9/9/97, in which you express your organization's desire to coordinate the participation of the telecommunications manufacturers. Law enforcement has met recently with telecommunications company representatives. However, the purpose of these meetings has not been to negotiate or request concessions from carriers. The intent of these meetings has been to work out differences that exist between law enforcement and the telecommunications industry regarding the proposed standard. Law enforcement views the proposed standard as missing basic capabilities to meet evidentiary and minimization requirements. These requirements are necessary to ensure the integrity and cost effectiveness of electronic surveillance.

The telecommunications carriers have assured us that they are in contact with their respective manufacturers regarding a CALEA solution for the specific platforms deployed in their networks. This approach is consistent with the standard business practice of the telecommunications industry, insofar that carriers communicate directly with manufacturers when interested in the development or implementation of a new feature.

Law enforcement is cognizant of the need for the telecommunications industry, both carriers and manufacturers alike to remain apprised of all significant developments that may result from the above described meetings. As such, law enforcement is willing to meet with all concerned parties in order to reach an amicable resolution to the issues under dispute.

Sincerely,

H. MICHAEL WARREN, *Senior Program Manager / Chief  
CALEA Implementation Section*

Mr. MCCOLLUM. Thank you very much, Mr. Flanigan.

Mr. Dempsey, let's see if we can get your testimony in before we have to run out to vote. Please, proceed.

**STATEMENT OF JAMES X. DEMPSEY, SENIOR STAFF COUNSEL,  
CENTER FOR DEMOCRACY AND TECHNOLOGY**

Mr. DEMPSEY. Mr. Chairman, members of the Crime Subcommittee, thank you for inviting me to testify today. The Center for Democracy and Technology is a civil liberties organization. Most of our current staff were involved in the drafting of this legislation. As the chairman indicated, at the time I was an assistant counsel to the subcommittee that had jurisdiction over this legislation and other members of our staff worked on the legislation. We still support the principles and goals of this legislation, but we cannot support it the way it is being currently implemented and interpreted by the FBI.

A number of the points that have already been made we agree with. I think there is consensus that the deadlines on this legislation cannot be met. The FBI basically admitted that in its implementation plan submitted in the Spring. There is also, I think, general agreement that the so-called punch list items—the additional items being sought by the FBI, the reasons why the FBI has so far blocked adoption of a industry standard—those add-ons go beyond the intent and scope of the legislation. They are additional capabilities which it might be nice to have, but they are not central to the core capability that Congress intended to preserve. They are enhancements, not preserving the capability.

There also, obviously, is need to re-address the question of reimbursement and the embedded base, the equipment that has been

installed since January 1, 1995, and I think there's a consensus on the need to address that, as well.

I would like to focus on the privacy aspects of this legislation because I think they are critical. One of the ironies of this entire debate is that the new technologies, while in some respects they make it harder for law enforcement to carry out wire taps, in many respects the new technologies make it easier. This is a powerful new technology. There is more information out there that people are putting on the airwaves and over the telephone lines, and the new technology in some respects is potentially more intrusive and more personally revealing. And this is coming about not as a result of CALEA, not as a result of congressional pressure, but simply as a result of the evolution and development of the technology.

Now, law enforcement is entitled to get those additional benefits, those enhancements in its capability. The question is, one, should they be mandated uniformly and ubiquitously throughout the country? And I think the answer is clearly "no, they should not." That was not the intention of CALEA to require an expansion of authority to the maximum allowed by the legislation.

The second very important issue is as those enhanced capabilities become available, what should be the legal standards that govern law enforcement access to them? Law enforcement can get them, but under what standards and rules? Are the standards strict enough to protect the privacy? We have always, as the wire tap laws have evolved from 1968 through 1986 with the Electronic Communications Privacy Act, through 1994 with CALEA, Congress has always said we need to ensure that the legal standards keep pace with the technology and that the rules and guidelines are adequate to protect privacy while allowing law enforcement a narrowly-focused access.

In several respects, I believe the technology has now already progressed beyond the protections that are in the law. One issue relates to location tracking in cellular telephone systems. During CALEA, there was a large controversy over location tracking, that is the ability of the cellular phone to identify the location of the user as the user moves from home to office, from one location to another. As it makes calls, those can be tracked. The FBI Director came before the subcommittee and testified that it was not the intention of CALEA to mandate a tracking capability as a uniform, nationwide requirement in wireless systems.

Under pressure from the FBI, the industry has acceded to that demand and has put that into the proposed standard. The standard that the FBI has rejected for other reasons has this additional capability, one which in our view clearly goes beyond the intent of CALEA. We believe that that should be stricken from the standard and we have petitioned the FCC to ask them to do so on the grounds that that violates the intent and goes beyond CALEA.

But regardless of whether tracking is in CALEA or out of CALEA, it is by and large coming. I think we probably have something like 30 million wireless telephone users in this country alone. That's probably even a low number. Thirty million ordinary Americans who carry wireless telephones with them. Those are basically tracking devices. You are carrying with you a tracking device. The Government can get access to that information. The question is

what is the proper standard, and we believe that that is so intrusive, in that you carry those phones into places where you're entitled to a reasonable expectation of privacy, the standard should be a probable cause standard.

The second aspect in which the standard goes beyond the requirements of CALEA and goes beyond preserving capability has to do with an emerging, somewhat esoteric, but critically important technology called "packet switching." The wire tap laws have always drawn a distinction between access to content and access to dialing or signalling information. The content of your communications are fully protected. Should I suspend?

Mr. MCCOLLUM. Mr. Dempsey, I think before you get into that very technical area we better go vote. Because we are going to have to have a recess. And so if you would suspend, we'll be in recess and we'll be back right after the vote is completed.

[Recess.]

Mr. MCCOLLUM. The subcommittee will come to order. If we can get started it would be helpful. Every time we have battles on the floor, I'm reminded of "order in the house" and know exactly where that expression comes from. When we had our recess commence for the vote a few minutes ago, Mr. Dempsey was in the middle of his testimony and about to give us a viewpoint of a somewhat technical nature on a point, and you may proceed, Mr. Dempsey.

Mr. DEMPSEY. Thank you, Mr. Chairman, and I'll try to make this as simple as possible. It's spelled out in greater detail, obviously, in my written testimony. But I think it is important to the whole future of the communications network in our country and critically important to this question of the proper balance between law enforcement and the standards that protect privacy.

I was saying that the laws have always drawn a distinction between content, which is fully protected, and the signalling or dialing or transactional information that routes the telephone conversation, which has always been less protected. The Supreme Court held that the dialing information has no Fourth Amendment protection at all. In 1986, in ECPA, the Electronic Communications Privacy Act, Congress did establish a very minimum requirement for access using what's known as a pen register or a trap and trace device to this dialing information that allows law enforcement to keep track of who is calling whom, which is an essential building-block of an investigation. Congress said that any prosecutor who goes to a judge and submits an application affirming that the information sought is relevant to an ongoing investigation, the judge shall sign that order. It's a mere relevant standard, no need for probable cause, no need even to suspect that the target is himself engaged in criminal conduct, but it is merely "relevant to"—he may be someone who was in touch with someone who was the target, and so on. It can get quite broad. Law enforcement, in fact, conducts ten times as many pen registers and trap and trace devices as it does wire taps.

The telecommunications system is evolving toward the use of something known as packet switching which takes every little communication, breaks it up into small packets of content, and attaches to each packet a little addressing information that tells the system where to send it. It gets stuffed into the pipeline where it

can be transmitted very efficiently at a high rate of speed and then, before it reaches its intended destination, the addressing information puts it all back together and you hear an uninterrupted conversation.

The question is how do we intercept these packets for law enforcement purposes? This was an issue that came up in the standards process and my understanding is it came up relatively late in the process. This is a just-emerging technology for telephony. It's been in the Internet for some time but for telephony it's just emerging. Many believe it's the future of telephony. The issue came up late in the standard-setting process and I have to say that basically industry and law enforcement punted on this one. They said, "We don't know how to sort this out. And if law enforcement has only authority for the dialing information, for the routing information, we don't know how to separate that from the content. Let's give everything to law enforcement." So basically, law enforcement would be getting under this mere relevance standard all the packets, not only the addressing information, but the content. And law enforcement would be relied upon to sort it out.

Now, in CALEA, Congress tried to use the technology, if possible, to enhance privacy protection. This was the two-sided balance of the legislation, to ensure that law enforcement got what it was entitled to and that a minimum access was preserved, but to try to ensure that law enforcement got no more than what it was entitled to. This whole packet switching issue completely destroys that dichotomy. And there are two possibilities.

One is to go back to the drawing board and figure out a way to separate, in this new emerging environment, content from signaling information so that law enforcement only gets what it's entitled to. The alternative is to simply say that if you're going to get all the content, you've got to meet the full probable cause court warrant standard under Title III.

Let me just conclude by saying that I think it would be a mistake to believe that the CALEA implementation problem could be solved merely by extending the compliance deadlines. I think it's critically important, as Congress always has before, when it addressed wiretapping, to not only look at the law enforcement needs, to not only look at the business needs and the cost issues, but to also look at the privacy issues. And that's why I am urging and CDT today is urging this committee in whatever you do, to also pay attention to the standard, because if there is, outside the purview of this committee, some sort of deal cut and the implementation of CALEA moves forward, but on a delayed timeframe as people recognize is going to have to be necessary, if it moves forward without addressing the question of the balance between law enforcement capabilities and the legal protections, then we will have lost a major opportunity here. This committee has to look at the standards for law enforcement access to this new technology and set the appropriately high standards necessary to protect privacy.

I'd be happy to answer any questions you have about the capacity requirements or further about the intent of the legislation. Thank you, Mr. Chairman.

[The prepared statement of Mr. Dempsey follows:]

PREPARED STATEMENT OF JAMES X. DEMPSEY, SENIOR STAFF COUNSEL, CENTER FOR  
DEMOCRACY AND TECHNOLOGY

I. INTRODUCTION AND SUMMARY

The Center for Democracy and Technology (CDT) is pleased to have this opportunity to testify about implementation of the Communications Assistance for Law Enforcement Act of 1994 (CALEA).

Our testimony will make the following points:

- CALEA is critically important to maintaining a balance among the interests of law enforcement, privacy and innovation as the nation's communications infrastructures continue to evolve and expand their importance in everyday life.
- Implementation of the legislation has gotten seriously off-track, largely because the FBI has departed from the reasonableness that marked the drafting of the law and instead has tried to use it to expand government surveillance capabilities.
- Congress has to intervene to make clear to the FBI that it cannot dictate the design of the nation's phone system and cannot insist upon industry acquiescence to capabilities that go beyond the status quo. Congress must intervene to return CALEA to a narrow focus on preserving but not expanding law enforcement access.

*Essential elements of the CALEA compromise*

CALEA was intended "to balance three key policies: (1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies." Judiciary Comm. Rep. 103-827, p. 13.

The essential features of the balance that Congress struck in CALEA were:

- (1) Telephone companies would be required to ensure that their systems continue to enable government agencies to intercept communications and associated call-identifying data, notwithstanding developments in technology.
- (2) Law enforcement's ability to wiretap would be preserved but not expanded.
- (3) Law enforcement would not be able to dictate system design; rather industry would develop the technical specifications for implementation, with an appeal to the Federal Communications Commission (FCC) if the standards process failed.
- (4) Privacy protections would be strengthened, especially to give added protection to the increasingly rich category of transactional or signaling data, and carriers would be required to protect the privacy of communications not authorized to be intercepted.
- (5) Carriers would be reimbursed for expenses in retrofitting existing equipment and adding additional capacity for law enforcement.
- (6) Mechanisms of accountability and oversight would ensure that the implementation process is open to review by Congress and ultimately by the public.

*CALEA is now in jeopardy.*

CALEA was adopted in October 1994. Three years later, implementation of the statute is in a state of uncertainty approaching paralysis and its carefully-crafted balance is in jeopardy:

To date, the FBI still has not issued a final capacity notice advising communications carriers how many simultaneous law enforcement surveillances they must be able to accommodate. The FBI's two efforts so far have proposed surveillance capacities far in excess of historical patterns. Capacity, though, was supposed to be the easy part of implementation. Congress thought it would take one year; it is now almost three.

In terms of the harder issue, defining technical standards to give service providers and their manufacturers a safe harbor for complying with CALEA's capability requirements, the FBI has tried to dictate the adoption of enhanced surveillance capabilities and has blocked adoption of an industry standard that did not include all the FBI's detailed proposals.

It appears that the FBI is trying to avoid reimbursement of carriers for the full cost of implementation, shifting costs to carriers, thereby avoiding responsibility for prioritizing law enforcement's needs and defeating the principle of accountability.

CDT and other public interest organizations have joined the cellular industry in urging the Federal Communications Commission (FCC) to take over implementation of CALEA. CDT has argued to the FCC that the proposed industry standard already goes too far in expanding law enforcement capabilities and fails to protect the privacy of communications not authorized to be intercepted.

Meanwhile, the October 25, 1998 implementation deadline for CALEA is rapidly approaching and the FBI is threatening to seek sanctions against any company that fails to meet its interpretation of the law.

*How did CALEA get so off track?*

Since CALEA was enacted, the FBI has tried to enforce the statute that it wanted, rather than the balanced and narrowly-focused statute that Congress enacted. Early versions of digital telephony legislation would have given the Department of Justice design control over the nation's telecommunications system. Congress rejected that approach. It instead enacted broad functional criteria and deferred to the industry standards process to develop solutions, with an appeal to the FCC if that process failed. FBI Director Louis Freeh testified in 1994 that this Committee's work was "a vast improvement" over the earlier version. Freeh testified that the revised bill was a "remarkable compromise," that it achieved "a delicate, critical balance." He emphasized that the legislation "reflects reasonableness in every provision."<sup>1</sup>

Since Congress finished its work, the FBI has rejected reasonableness. It has sought to dominate the industry standards process and has sought to assume for itself the type of design control over the nation's telecommunications system that Congress expressly denied it. The FBI has tried to use the statute to exploit the potential of the new digital technology to enhance rather than merely preserve its surveillance capability.

*—What can Congress do now?*

CDT is a privacy and civil liberties organization focused on promoting democratic values in the new digital media. Much of the current staff at CDT were involved in the development of CALEA. I myself was assistant counsel to the Subcommittee that originated CALEA in the House, and I spent considerable time on this legislation. Having helped put this statute together, we cannot support it the way it is being implemented.

CDT does not question here the objective of preserving a narrowly-focused ability for the government to carry out electronic surveillance in the face of ongoing technological changes. Nor do we question here that wiretapping is a useful law enforcement tool, although we suspect it is not as critical as the current leadership of the FBI claims. Finally, we do not ask the Committee today to block the government from taking advantage of market-driven changes in technology that enhance surveillance. (One of the ironies of the CALEA debate is that digital technology in many ways enhances law enforcement's abilities.)

Instead, we urge the Committee to return the CALEA implementation process to the spirit of reasonableness that characterized the drafting and enactment of CALEA. We urge the Committee to ensure that CALEA is not interpreted as a mandate to industry to affirmatively design a surveillance infrastructure, but merely as a requirement, in the words of FBI Director Freeh, to "preserv[e] that tool as it has existed since 1968." Hearings, p. 113. And because developments in technology are in some ways making surveillance easier, we urge the Committee to strengthen, not weaken the wiretap laws, to protect the privacy of innocent citizens.

CALEA is heading for the proverbial trainwreck. In October 1998, the legislation takes effect. Standards for implementation have not been adopted. Even if adopted tomorrow, they could not be incorporated into equipment until sometime in 1999 at the earliest. The FCC, however, is clearly reluctant to become involved in the matter. This means that, in October 1998, if not sooner, the statute could be thrown into the courts, with serious risks for law enforcement, industry and privacy.

It is clear now that it is time for Congress to intervene to reassert the balance that it intended in 1994. It can do so without reopening the entire statute. The goals of Congress should be to make it clear that the FBI cannot dominate the implementation process and that the FBI's proposals for enhanced surveillance capability are beyond the mandate of CALEA.

<sup>1</sup>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. (1994) (hereinafter "Hearings") pp. 112-14.

- Congress can achieve these goals by directing the FBI to begin promptly to reimburse carriers to implement the proposed industry standard minus location tracking and the packet switching option and minus the other additional items still sought by the FBI.
- Alternatively, Congress can amend the language of CALEA section 107(b) to require the FCC to institute a rulemaking on standards.
- In light of the delays caused by the FBI, it seems necessary for Congress to extend the October 25, 1998 implementation deadline and the reimbursement cutoff date of January 1, 1995.
- Congress should make it clear that location information is not a CALEA mandate, but because location tracking information will probably become increasingly available and increasingly specific within wireless systems, whatever is done in terms of CALEA implementation, Congress should amend Title III to enact a probable cause standard for access to location information.

## II. CALEA OVERVIEW—WHAT DID CONGRESS INTEND?

For much of the history of telephony, the government's ability to wiretap was an unintended by-product of the design of the telephone system, and that capability remained largely static. More recently, the technology has been changing rapidly. In this time of rapid development, the industry could ignore law enforcement concerns, and design its systems only to meet market demands most efficiently, in which case some changes would enhance government surveillance capability and others would hinder it. At the other extreme, industry, if mandated, could build a comprehensive surveillance network. There is a middle course: society could try to achieve a balance, preserving a narrowly focused surveillance capability while protecting privacy and not impeding the development of new services to meet customer demands.

In CALEA, Congress chose this third path of balance. The law was intended to ensure that developments in technology did not have the unintended effect of eroding government surveillance capabilities. It is clear that Congress did not intend to mandate that the technology be developed in ways that would maximize its surveillance potential. The Judiciary Committee report states that CALEA was intended "to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts" (emphasis added). FBI Director Louis Freeh testified repeatedly and consistently that the legislation was intended to preserve, not expand the capability as it had existed since 1968. This Committee's report stressed that CALEA's requirements were to be narrowly construed.

In determining how far the FBI approach to CALEA implementation has departed from Congress' intent, it is useful to look at the actual problems that were presented to Congress. Between 1992 and 1994, the FBI conducted a series of surveys of federal, state and local law enforcement agencies and found 183 technology-based problems out of the tens of thousands of surveillances conducted. (The problems covered both Title III content interceptions and the interception of call-identifying information through pen registers and trap and trace devices.)

Of the problems identified by the FBI, the most common was lack of adequate capacity in cellular systems to accommodate multiple surveillances at the same time. This accounted for 30% of all problems law enforcement could identify. The second most common problem was the inability of certain cellular systems to provide law enforcement with call-identifying information on a real-time or contemporaneous basis. (The cellular system collected dialing information, but there was a delay before the information could be accessed.) The third most common set of problems related to special dialing features. Basically, when a person uses speed dialing, voice dialing or automatic redial or call-back, the pen register on the customer line only picks up the coded command, not the full number that it represents. The fourth most common problem was call forwarding. Law enforcement could not capture incoming calls to the target's line that were forwarded at the central office using a service provided by the telephone company. Like the other problems, call forwarding was not a uniquely "digital" problem; it had existed in the analog world. There were other miscellaneous problems. See Judiciary Comm. Rep., p. 15.

From this survey, it was clear to Congress that there were problems meriting legislation. And, of course, Congress was concerned to ensure that the future evolution of technology did not create new problems. But it was a fundamental assumption of Congress in 1994 that most equipment in place at the time was able to meet law enforcement surveillance requirements. After all, of the tens of thousands of wiretaps, pen registers and traps and traces conducted in the 1992-94 timeframe, there had been only 183 documented problems. This type of record cannot serve as the basis for a comprehensive redesign of the nation's telecommunications system.

Conclusive evidence that Congress' assumption was correct is found in the fact that since 1994, even though CALEA implementation has been stalled, even though industry has continued to install equipment not designed with law enforcement's requirements in mind, electronic surveillance continues to be carried out. In the years since CALEA was enacted, the numbers of wiretaps, pen registers and trap and trace devices have remained at all-time highs, while the number of persons intercepted and the number of conversations monitored have gone up. There is no need for a comprehensive redesign of the telecommunications networks. Most equipment and services in place today are "CALEA compliant."

### III. PRIVACY PROBLEMS RAISED BY CALEA IMPLEMENTATION

Despite the discrete nature of the problems identified by the FBI and presented to Congress in 1994, and despite evidence that the nation's telecommunications system continues to support law enforcement wiretaps, the FBI has pushed for a comprehensive redesign of communications infrastructures. The FBI dominated the industry standards setting process. Under pressure from the FBI, industry yielded, and put forth a proposed standard that expands surveillance capabilities and fails to protect the privacy and security of communications not authorized to be intercepted.

Two provisions of the industry proposed standard are of major concern:

#### A. Location Tracking

The FBI wants to require wireless carriers to provide law enforcement agencies with location information at the beginning and end of any cellular and PCS communication, thereby turning the nation's wireless phones—now used by millions of ordinary citizens—into real-time tracking devices. 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 location or tracking requirement.

At the first joint House and Senate hearing 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. Freeh was very clear in disavowing any intent to cover 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 tracking information." Hearings, p. 6.

Wireless phone tracking was a very potent source of opposition to CALEA. The FBI was eager to put it off the table. Nothing in the subsequent negotiations over CALEA brought it back in. When FBI Director Freeh returned to Congress to praise the revised CALEA bill, he never mentioned tracking. Ever since the law was signed, the FBI has worked mightily to claim that tracking is a CALEA mandate, and industry, while never agreeing that it was a mandate, put it in the standard.

#### B. Packet Switched Content Delivery

Telecommunications companies are beginning to incorporate in their systems "packet switching" protocols similar to those used on the Internet. 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.

This development has potentially profound implications for government surveillance. It has always been assumed that there is a distinction between call content, which is entitled to full Fourth Amendment protection requiring a judicial warrant based on probable cause, and signaling information, which is protected under a much lower relevance standard. In CALEA, Congress required companies to use technology that kept these two separate. But in the CALEA process, industry and the FBI assumed—apparently with little study—that it is not feasible to provide signaling information separate from the communications content in a packet switching environment. Therefore, the FBI and industry have proposed a standard that allows companies to deliver the entire packet data stream—including call communications—when law enforcement is entitled to receive only dialing or signaling information under a pen register order. The proposed standard relies on law enforcement to sort out the addressing information from the content, keeping the former but ignoring the latter.

This approach, were it followed, could well represent a total obliteration of the distinction between call content and signaling information that was a core assumption of the Electronic Communications Privacy Act of 1986. It also 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."

Before casting aside a basic distinction of the wiretap laws, there should be a careful technical examination of whether call-identifying information can reasonably be separated from the full data packet. The implementation of CALEA could go forward without a packet-switching standard. A technical inquiry, by the FCC or another entity, undertaken at the direction of Congress, could examine the privacy and security aspects of packet switching and determine whether, and if so how, call content can be withheld from the government when the government is not authorized to receive it. Otherwise, Congress should act to make it clear that the government can access packet data information only in response to a Title III order, not in response to a pen register order.

#### C. Additional Surveillance Enhancements Sought by the FBI

In the foregoing respects, the standard proposed by industry under FBI pressure 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. The FBI's "punch-list" of enhancements includes:

- *Multi-party monitoring*—The FBI wants phone companies to design their systems so the government can 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, but the FBI wants to continue monitoring those left behind after the subject of the court order is no longer on the call. Not only is this not mandated by CALEA, but providing it would violate section 103(a)(4)(A) of CALEA and the particularity requirement of Title III and the Fourth Amendment, 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.
- *Expanded definition of call-identifying information*—Much of the controversy under CALEA relates to the distinction between interception of call content and the interception of call-identifying information. Call-identifying information is collected with pen registers or trap and trace devices, authorized without probable cause and without the discretionary review accorded to full call content interceptions. The FBI is seeking an expanded definition of "call-identifying information" in order to increase the amount of information that it obtains under the minimal standard applicable to pen registers.

But CALEA rejected this approach. 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). Other signaling or sounds that do not relate to dialed numbers are neither encompassed by the pen register law nor required by CALEA. Contrary to this intent, the FBI wants to use pen registers to collect digits that the subject dials after cut-through. These digits do not identify a call in any sense but rather are content-related. The FBI is also seeking on-line notifications of customer changes in service, messages indicating when a party puts a call on hold, and messages indicating when the subject has a voice mail.

#### D. Capacity

One of the major issues that prompted Congress to adopt CALEA was concern that telephone switches would not have the capacity to conduct multiple simultaneous intercepts. This had already been a problem in cellular systems, especially in New York City, where a number of law enforcement agencies operate and were competing for a limited number of surveillance ports on cellular switches.

Since law enforcement surveillance activity obviously varies from region to region, CALEA requires the FBI to issue notice of its capacity requirements for each geographic area, so that carriers know how much capacity to install. In October, 1995, the FBI issued its first proposed capacity notice. It seemed to require companies in major cities to install a surveillance capacity that would allow simultaneous mon-

itoring of up to 1% of customer lines in service. This proposal was roundly criticized as excessive and the FBI withdrew it.

In January, 1997, the FBI issued a second notice, using a new methodology based on past activity. However, this second notice was also deficient in three ways:

- (1) The FBI exaggerated law enforcement's past experience. The Bureau collected data, consisting of combined federal, state and local law enforcement surveillance activity for each county or service area nationwide, between 1993 and 1995. From this data, the FBI determined the 24-hour peak of surveillance activity for each switch, over the course of the 26 month survey period. From switch to switch, these peaks did not occur on the same day, but the FBI added them together to obtain a hypothetical county-wide "peak," which the notice requires companies to meet as if the surveillances occurred all on the same day.
- (2) The second notice and some of the FBI's informal comments about it have seemed to imply that each and every carrier serving a particular area would have to install capacity sufficient to meet the total surveillance needs for that region, even if the carrier only served a portion of the customers in the area. Even broader interpretations of the notice, which the FBI has informally disavowed, would require carriers to install in each switch a capacity sufficient to meet the requirements projected for an entire county or multi-county service area. Under either of these interpretations, the requirements of the second notice would require industry to install capacity unrelated to historical surveillance activity, costing taxpayers many millions of dollars in unnecessary reimbursement.
- (3) The second notice draws no distinction between the capacity required to intercept call content and the capacity required to access dialed number information, even though CALEA requires a distinction between interceptions of call content and interceptions of call-identifying information through pen registers or trap and trace devices. The FBI indicates that 90% of all surveillances involve access only to dialed number information, not call content. The distinction is important for privacy because the capacity to intercept call content is more intrusive (and may be more expensive) than the capacity to intercept call-identifying information. Congress wanted companies to use technology that limited the amount of information provided to law enforcement under pen register and trap and trace authority. The second notice ignores that intent.

Given the lack of any official written interpretation of the notice that is subject to public review, we have concluded that the problems created by the conflicting interpretations of the second notice are so profound that the FBI should issue another notice for further public comment, making it clear what capacity levels were intended.

#### IV. STRONG PRIVACY PROTECTIONS ARE ESSENTIAL TO THE INTEGRITY OF CALEA

CALEA was based on the dual premise that the laws authorizing electronic surveillance have strict legal requirements to protect privacy and that those standards are strictly enforced by the courts. In the absence of such strict legal requirements—if they are weakened legislatively or if they are not enforced by the courts—then the premise of CALEA falters and the legislation becomes far more threatening, requiring as it does the ubiquitous preservation of easy technical access.

Unfortunately, since CALEA was enacted, the Justice Department has sought numerous weakening amendments to the wiretap laws. Congress so far has rejected most, but it included two weakening changes in the 1996 terrorism bill. There, the Justice Department won Congressional repeal of one of the privacy enhancements adopted in CALEA with the intent of balancing privacy concerns with law enforcement needs (the now-repealed provision extended the privacy protections of the wiretap laws to wireless data transfers). In addition, this Committee inserted a provision carving electronic funds transfer information out of the definition of electronic communication. In the Senate, there was a proposal to carve out wiretapping in prisons. Further, the Justice Department continues to pursue other amendments that would loosen the privacy standards of the wiretap laws, notably the standards for roving taps.

Some clarifications in the wiretap laws may be warranted. But it undermines the foundations of CALEA if those changes weaken the existing privacy protections, or if those protections are not working as intended to limit investigative agency discretion. Unless Title III, ECPA, and the pen register statute constitute meaningful privacy legislation, the foundation of CALEA will be eroded.

If this Committee supports CALEA, it should support strong privacy provisions in the wiretap laws. Continuing technological developments are already shifting the balance in law enforcement's favor. Wireless telephone systems are developing the capability to provide more refined location information on wireless phone users. Nonconsensual government monitoring of location through a wireless phone implicates privacy interests. Since wireless telephones are regularly carried into places where a person has a reasonable expectation of privacy, Congress should clarify the law by requiring a warrant based on a showing of probable cause for nonconsensual governmental access to real-time wireless telephone location information.

Advanced signaling systems have also blurred the distinction between call-identifying information and call content. CALEA was intended to ensure that pen registers and trap and trace devices only collect signaling information utilized in call processing. It appears that that is not happening. Instead, it appears that more and more information is being handled on the signaling channel, subject only to the low pen register standard. If that is the direction of the technology, then Congress should amend the standards for governmental access to signaling data to require a judge to make an affirmative finding, based on a showing by the government, at least that the information sought is relevant and material to an ongoing criminal investigation.

#### V. CONCLUSIONS

There is a significant difference between what law enforcement thinks would be a useful capability versus what is essential to allow law enforcement to carry out surveillance as it has since 1968. There is a significant difference between authorizing law enforcement to take advantage of whatever capabilities are available as a result of market-driven developments versus using the power of the government to require industry nationwide to build a telecommunications system that optimizes the surveillance potential of the technology. In CALEA, Congress did not say that the FBI could require phone companies to design their systems to provide to law enforcement all the capabilities that could be technically produced. Rather, Congress said that the companies had to preserve a minimal capability.

Therefore, Congress should intervene to get the CALEA process back on track. It can do so directly, by authorizing the FBI to begin reimbursing carriers to implement the industry standard, minus tracking and packet switching, or Congress can require the FCC to exercise its rulemaking function and decide the petitions now before it. But it has to be made clear that the law does not allow the FBI to use the reimbursement process or the industry standards process to write its own demands into the network design. Congress will have to extend the deadlines, so that the FBI cannot use the pressure of October 1998 to force industry to capitulate. And Congress must make it clear that the government is responsible for reimbursing industry to retrofit existing equipment, including equipment installed after January 1, 1995. This will force the FBI to prioritize its requests and will keep the funding issue in the public light, rather than shifting the costs to the companies, where they hidden in the phone bills of consumers.

Regardless of the outcome of the CALEA implementation debate, it is clear that technology is moving in directions that increase government powers. Congress should ensure that those powers are carefully controlled. For this reason we urge the Committee, regardless of the outcome of the CALEA implementation debate, to establish a probable cause standard for access to location tracking information and a more meaningful standard for access to other signaling information.

#### ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY

CDT is an independent, non-profit public interest policy organization. The Center's mission is to develop and implement public policies to protect and advance individual liberty and democratic values in new digital communications media. The Center achieves its goals through policy development, public education, and coalition building. CDT coordinates the Digital Privacy and Security Working Group (DPSWG), a forum of more than 50 computer, communications, and public interest organizations and associations working on communications privacy issues. Members of the Working Group played a critical role in ensuring that CALEA included privacy protections and public accountability mechanisms and was narrowly tailored so as not to impede the deployment of new technology.

House Rule XI, clause 2(g)(4) disclosures: Neither James X. Dempsey nor the Center for Democracy and Technology have received any federal grant, contract or subcontract in the current or preceding two fiscal years, nor do they represent any entity that has received any federal grant, contract or subcontract in the current or preceding two fiscal years.

## FOR MORE INFORMATION CONTACT:

James X. Dempsey, Senior Staff Counsel, Center for Democracy and Technology

+1 202.637.9800 (v)

+1 202.637.0968 (f)

jdempsey@cdt.org

<http://www.cdt.org/>

Mr. MCCOLLUM. Thank you very much and thank all of you for your testimony. And we'll go to rounds of 5-minute questions under the 5-minute rule and I will recognize myself for the first round of 5-minute questions. Mr. Flanigan, you had expressed concern over the voting that eventually took place on the standards that went out and they were voted down the first time and they're out again in a different version this time. How did the FBI have the power to veto these standards? How did they have the power to vote? I don't understand that. Can you explain that a little bit more?

Mr. FLANIGAN I'd be happy to, Mr. Chairman. The—When a document goes through its formulating group, the process allows the formulating group to determine whether it's going to go as an ANSI ballot or whether its going to go as something other than that.

At that point, back in the spring of 1997, the formulating group decided to go as an ANSI ballot.

Mr. MCCOLLUM. What's an ANSI ballot?

Mr. FLANIGAN ANSI is American National Standards Institute. That's who has granted TIA the authority to become what you call an SDO.

Mr. MCCOLLUM. Fair enough.

Mr. FLANIGAN And so we have the rights to carry this process through. At that time, the vote is open to all interested parties. The FBI is an interested party. All Government bodies would be an interested party. So the ballot went and we get the response back and we work on consensus. If I recall, the votes were about 94 votes back and there were 39 "nos." And out of the 39 "nos," at least 30 were the identical documents of people who never even attended a standards meeting.

Mr. MCCOLLUM. So you're talking about DEA having a vote, local law enforcement having a vote. Who all would have gotten these ballots?

Mr. FLANIGAN These were all law enforcement agencies around the United States, as well as the FBI.

Mr. MCCOLLUM. So, state as well as Federal?

Mr. FLANIGAN That is correct.

Mr. MCCOLLUM. So—

Mr. WHEELER. Mr. Chairman?

Mr. MCCOLLUM. Yes?

Mr. WHEELER. Can I help, perhaps, on that point just a little bit?

Mr. MCCOLLUM. Mr. Wheeler, sure.

Mr. WHEELER. This is an example—happens to be from Pinellas County, Florida. The sheriff there, Everett S. Rice, who filed this document which is his opposition to the standard. To the best of my knowledge, Mr. Rice or his representatives never attended any of the meetings, but in the process, he was kind enough to also file the letter which he received asking him to file, which says that "all questions should go to Special Agent Michael McDowell," and cites the activities of the Telecommunications Enforcement Unit at the

FBI, and then to submit as his submission the FBI's submission. And—I mean, this perhaps answers your question as to where those votes came from. The Sheriff was kind enough to help us track that down.

Mr. MCCOLLUM. Well, I appreciate that. Will that be part of the record?

Mr. WHEELER. I'd be happy to make it part of the record.

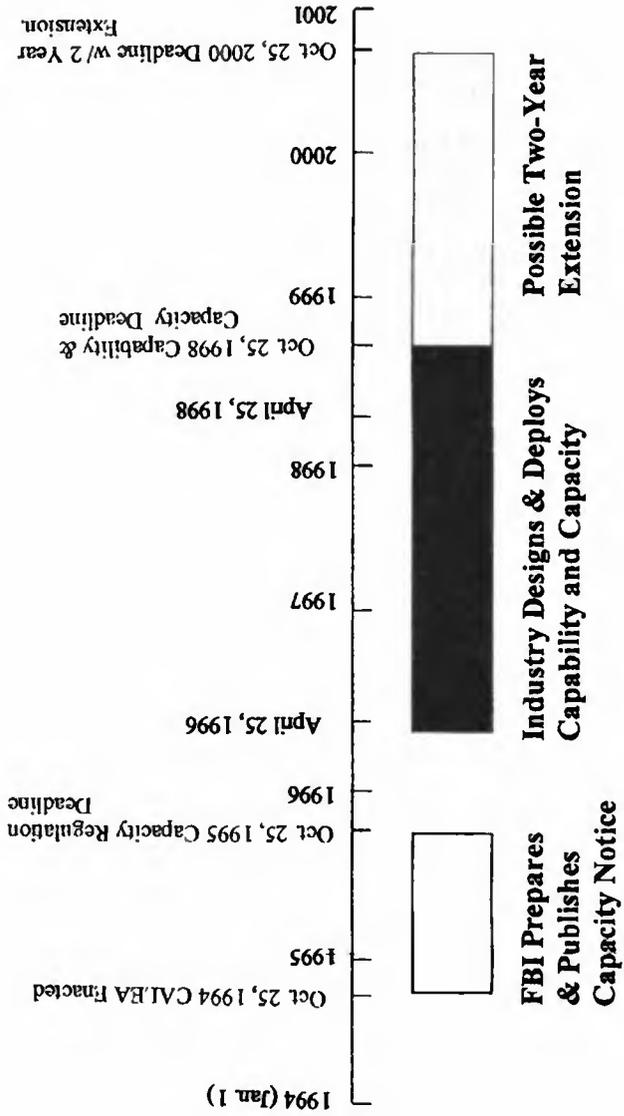
[The information referred to follows:]

# Lead Time Required To Design And Deploy A CALEA Standard



- Design and Build Necessary Software and Equipment
- Critical Market Deployment

# Intended Implementation of CALEA



Mr. MCCOLLUM. Thank you. Mr. Flanigan, how many carriers voted no?

Mr. FLANIGAN How many carriers voted no?

Mr. MCCOLLUM. Yes, sir.

Mr. FLANIGAN I believe zero carriers voted no.

Mr. MCCOLLUM. All right. Now, you said there's an option that ANSI—

Mr. FLANIGAN Excuse me, I'm being told that—

Mr. WHEELER. I think there were a couple of carriers who voted no, Mr. Chairman—

Mr. FLANIGAN That is right.

Mr. WHEELER. On the basis that, with respect to the location issue. They felt that it exceeded surveillance that was authorized in CALEA. But the "no" votes were only 3 out of 30 some. So an overwhelming majority of the carriers supported the standard.

Mr. MCCOLLUM. But my understanding if correct, Mr. Flanigan, is that this was a procedure that was adopted, but it could have been a procedure—a different procedure adopted. The statute did not require this particular technique, is that right?

Mr. FLANIGAN That is correct. We've gotten back the comments from that first ballot, and we have addressed those comments. Many of the concerns have been readdressed, gone back to the committees, and now we have resubmitted the ballot again under ANSI. But in addition, we've also put out what we call an "interim standard" ballot. This is a separate standard which happens to be identical to the ANSI standard. However, the interim standard can only be voted on by the industry or the people who are willing to pay to be at the table.

Mr. MCCOLLUM. So you've got a dual track going on?

Mr. FLANIGAN Right now, we have a dual track going on. Both of these votes are due back at the end of this month. It is the intent, as I said earlier, that if this interim standard passes to begin work on that standard. An interim standard is defined as a standard that's out there as a test standard. Each year it has to be revalidated, and after 3 years the interim standard would have to be converted to an ANSI standard.

Mr. MCCOLLUM. In other words, eventually the Sheriff in Pinellas County is going to get to vote on this no matter what.

Mr. FLANIGAN He will not be allowed to vote on the interim standard, unless—

Mr. MCCOLLUM. But ultimately, you said after 3 years it has to go out as an ANSI.

Mr. FLANIGAN That is correct. You are correct, sir.

Mr. MCCOLLUM. So eventually he'd have to vote on it.

Mr. FLANIGAN That is correct.

Mr. MCCOLLUM. Now, is that required by statute, that we do it this—that ultimately there be an ANSI standard vote?

Mr. FLANIGAN No, it is not required by statute.

Mr. MCCOLLUM. All right. My understanding is, in fact, the statute says that even if you don't get any standards you have to have CALEA compliance at the end of the drop dead date in October, 1998. Is that not true, Mr. Wheeler? Mr. Kitchen?

Well, the statute actually says that by October 1998 you have to have CALEA compliance, even if you don't have a standard.

Mr. WHEELER. It is our understanding of the law that failure to have a standard does not excuse carriers from complying with CALEA.

Mr. MCCOLLUM. But what I want to know is without a standard can this act be complied with? Is it technically or practically possible to comply with the act on the part of the carriers and the other parties to this without a standard?

Mr. FLANIGAN Mr. Chairman, let me try and answer that. It is not technically possible today because we have gone beyond the date which allows the time for any manufacturer to build into its switch the ability then for a carrier—

Mr. MCCOLLUM. But if we extended the date, could it be complied with without a standard?

Mr. FLANIGAN That is—yes, it can be. If the companies, the individual manufacturers, are willing to decide on their own to build a product which they believe may be compliant.

Mr. MCCOLLUM. I'll let you all answer, but then I'm going have some more questions. Mr. Neel?

Mr. NEEL. Well, just very briefly. I think the point is that if you do this unilaterally, you're guessing. And by guessing you're opening yourself up for some severe litigation.

Mr. MCCOLLUM. All right. Mr. Kitchen?

Mr. KITCHEN. From a practical standpoint, if you don't have a standard as to how these switches are going to be constructed and designed, you could conceivable end up with a situation that wire taps would be done one way in New York and a different way in LA and a different way in Washington, D.C. And I think that would be a tremendous burden on the law enforcement people if there wasn't some consistency in how they go about achieving their goals.

Mr. MCCOLLUM. Mr. Dempsey?

Mr. DEMPSEY. Mr. Chairman, actually I guess I would disagree with that last point a little bit. I don't think that there is a problem with doing wire taps differently on different systems, so long as a base capability is provided. That was the intent of CALEA. In CALEA Congress tried to make it clear that there is not one technical solution, not one specific way to do this. I think what has happened, and the answer to your question is, who decides what is compliance? A lot of the dispute here has been over the FBI's claim that it is the sole repository of authority on what is compliance. I think that there are probably many systems out there today which are essentially compliant.

Mr. MCCOLLUM. Well, I don't want to belabor my time here, but it appears to me just from listening to you gentlemen that, again, without hearing the FBI which we'll hear in a few minutes, that they have not decided on what's solely compliant, they're simply using the political tools that you've given them, or that the group involved in this consensus building chose to give them, using ANSI standards. They went out and stuffed the ballot boxes, but did it legitimately. That's what it sounds like. I'm not saying that's right or wrong, but—

Mr. DEMPSEY. Well, at some of these meetings, it's my understanding that the FBI has said that if you don't meet the ESI, this

Electronic Surveillance Interface, their written definition, that they will consider a carrier non-compliant.

In regards to stuffing the ballot box, I guess I would have to say that the drafters of the legislation did not intend that there would be that ability. The legislation does say an industry association or standard-setting body, and the FBI and law enforcement generally were to be given a consultative role. It clearly went far beyond the consultative role into the "take it or leave it" role, and that's contrary to the intent of the legislation and that's what's put us in this posture.

Mr. MCCOLLUM. I've got to go on, but Mr. Flanigan, when are you—a very quick comment.

Mr. FLANIGAN The purpose was really to try and reach consensus. And that was the purpose of letting the FBI sit at the table, have a vote, and it just has not worked.

Mr. MCCOLLUM. Mr. Meehan, you're recognized for 5 minutes.

Mr. MEEHAN. Thank you, Mr. Chairman. Mr. Neel, while the industry's proposed standards implement about 90 percent of the capabilities requested by the FBI, there are ten or so capabilities that the FBI demands but the industry considers either technically these are not required by CALEA. You were talking in your testimony—if the industry were to accept standards contained in these contested capabilities, how would this add to the cost of compliance with CALEA? Now, base on your testimony today, for example, is it your opinion that this would double the cost of CALEA compliance? Could you—well let me just ask, would it double the cost?

Mr. NEEL. Well, first of all, we don't know what the cost would be to double. If you're looking at the appropriated, or the authorized funding level of 500 million dollars, our own assessment is that it could run up to 1.2 billion dollars as I testified to simply bring three switches into compliance for wired carriers. This does not include other wireline switches or the wireless carriers, so it could be vastly in excess of that. And on the low end could be around 500 million.

Now, the punch list, the so-called ten items in dispute, we believe the cost—and again, these are our estimates—could be between 217 and 602 million dollars just to comply with those ten disputed items, which is about double what we already have agreed to, the base-line compliance standard.

Mr. MEEHAN. Like me ask you another question. We talked about the October 25th, 1998 deadline and the possibility of facing daily fines up to \$10,000 in the absence of consensus on capability standards. Non-compliant carriers would escape these sanctions for up to 2 years by convincing the FCC that the compliance was not reasonably achievable through the application of technology available within the compliance period.

Assuming that the carriers will not be able to meet that October 1998 deadline for compliance with CALEA's capability requirements, a point which you emphasized in your testimony, how likely is it that they could avoid sanctions by arguing that the compliance was not reasonably achievable for a lack of adequate technology?

Mr. NEEL. Well, we haven't had a lot of luck with this Federal Communications Commission on any issue, so I'm not sure how to

project here. But let's just say—well, certainly we would be forced to do that.

Mr. MEEHAN. You must have considered that, though, in considering—

Mr. NEEL. Oh and we will be forced to do that. But if you step back to what we all want, which is to get the standards done and get agreement on the standards early and get this implemented as soon possible, then that would lift a lot of this litigation possibility here.

We would obviously love to be able to get this all done by October 1998 and at a cost far below the money that the taxpayers are going to have to spend. But it is not realistic at this point. So we will have no choice but to petition anybody possible to extend this deadline and to keep negotiating and to keep trying to make this work.

Mr. MEEHAN. Let me ask any member of the panel, obviously we're aware that negotiations between the industry and law enforcement have certainly made some progress ever since main Justice has assumed a more active role, it seems to me, in the discussions. And there were high-level meetings that occurred as recently as yesterday. I'm wondering if you, any of you, could brief the subcommittee on the status of negotiations as of this moment. Is it fair to say—is a deal imminent, likely in the upcoming weeks, nearly possible at some future date, or doubtful, or are we in a position where we're going to use this hearing to kind of get members of this committee involved to try to force the issue? I'm just wondering exactly where we are. I do think it's important to also mention that I believe that this hearing should be—should not be confrontational, in terms of—I think there at a meeting with the Appropriations Subcommittee Chair, Representative Rogers, and the chairman indicated that he wants this settled, and both sides to get together and strike a deal as soon as possible. Where are we with that?

Mr. NEEL. Well, I would just suggest—I think of all the options you mentioned, we're at number three and number six. Number three is that it is possible at some future date and number six is that it's important that this committee impresses upon the FBI what its role really should be under the act, as Jim mentioned, and others. We want this done yesterday. We have no incentive for footdragging whatsoever, but frankly, we are petitioners to a certain extent. We don't have the kind of leverage in this process when law enforcement is sitting on the other side of the table. So we would be hopeful that you would exert some of that leverage to make sure that they do get to a solution on this and that they are reasonable in their expectations on capacity capability and cost.

Mr. MEEHAN. Mr. Wheeler?

Mr. WHEELER. Mr. Meehan, let me see if I can anticipate one of the issues in the effort to resolve this. Because it is an issue that is—that bears on the responsibilities of this committee, the authorizing committee, and that is what is in CALEA and what is out of CALEA. Now, you're going to hear, I would suspect, in the next panel, a suggestion that there be the so-called toggle installed, which means that well, we'll take all the things over here that we've agreed on thus far, but we also want you to build all the

things on our punch list and then if they're determined to be legal we want you to have a toggle in the software that turns them on.

And there are two problems with that. Number one, as Roy has just testified, it's going to take the price and at least make it 2X, if not higher, for things that don't need to be in standards. And number two is that we're talking about issues that are outside of what this committee said should be the scope of the law, so toggle or no toggle, they are still outside.

If this committee could simply state that "here are the four corners of what we expected to see happen in CALEA and the resolution needs to occur inside those four corners," I think it would go a long way to speeding up the process and allowing us both to focus on what is achievable and should be achieved.

Mr. KITCHEN. Let me respond as far as the need to move quickly on this. The PCS industry is the new entrants here, and our members are putting in switches daily. They're ordering them daily. And what they face right now is ordering a switch that they have no idea whether it's going to comply with this future standard unknown or not. And they're having to invest hundreds of millions of dollars in these switches with the possibility that they could have to turn around and retrofit them in a very short period of time with no hope, with the January 1, 1995 date in place, of ever getting any refund from the Government. And I think that's a very important issue and that's why our members are very anxious to get this resolved. So time is of the essence.

Mr. NEEL. Let me just comment on the standards side of it. I am confident that the interim standard that we now have out for a ballot will be passed and within the next few months we will be able to recommend to the manufacturers that this standard meets CALEA 100 percent. In addition, we have committed to working with the FBI very closely for the next several weeks, whatever it takes. And mentioning your meeting yesterday, we were actually given a deadline that we better have some things ready very shortly—that we are going to meet this deadline of getting the punch list items reviewed and, if necessary, consider an additional capability and some additional funding would probably be required for those.

Mr. MCCOLLUM. Thank you, Mr. Meehan. Mr. Buyer, you're recognized for 5 minutes.

Mr. BUYER. Thanks, Mr. Chairman. I recall back when we were putting together the telecommunications bill, Congress really wanted to move—let the industry and the FBI and law enforcement work it out. And I guess that's what we're watching and observing right now, that the working out has not been easy. We kind of knew that as we're moving from the analog to digital and there's a lot of things we don't completely understand and the science is forever moving and standards which we may set today—it's going to be a constantly moving target on that technology, and hopefully this relationship for which is difficult today evolves, because this will be a continuation as the technology continues to move.

I look at this when you requested about identifying the four corners of the document, I thought we did that in the act itself. We run into little spats even with the FCC when we ask them not to create regulations and we put right in the law "do not write regula-

tions regarding X, Y, and Z" and what's the FCC do? They go out and write regulations regarding X, Y, and Z. And it requires courts to tell them, "you didn't read the act." So I thought we did that. So I thought that we laid out clearly that the act requires the telecommunications industry on the issues—you have to enable intercept, enable the access, provide the intercept communications, the information to the Government, and require the carriers to do in fact that intercept. Makes it clear.

Then it also turns to the FBI and tells the FBI what you can't do. The act tells law enforcement "you're not authorized to require any specific design of equipment, facilities, services, features, systems, configurations, nor can the Government prohibit the adoption of equipment, facilities, services, feature provided by any manufacturer." So let me ask you, what do you need from us? Do you need for us to be a little clearer hear?

Mr. DEMPSEY. Congressman, if I may, I think what is necessary here is for Congress to make it clear to the FBI that they cannot do what they're doing now, which is to hold out the threat of a \$10,000 a day fine and a court action in order to gain additional concessions.

This negotiating process that people talk about now, I have to say, I think people are a little naive if they think this is the end of the process. As you said yourself, the technology is changing. If the FBI is able to drive industry to the wall on these 10 items, or get 5 of 10, or 6 of 10, or whatever is the deal, throw a little money into the pot, and extend the deadline, in 2 years or in 5 years there's going to be another technology, and the FBI is going to come back and say "this technology is not CALEA-compliant. Do it this way." And there will be another punch list. And there will be more pressure on industry to make further modifications that amount to enhancements, that amount to efforts to exploit the potential of the technology to increase the surveillance power, rather than to merely maintain the base.

Mr. WHEELER. Mr. Buyer, Jim is exactly right. But let me give you a specific example to the issue that you raise. This is the Electronic Surveillance Interface document that the FBI presented and said "take it or leave it. This is what you have to do." And here is what it says on the first page. "In essence, telecommunications carriers that follow the recommendations and requirements herein for the ESI would find a safe harbor under CALEA with regard to this aspect of electronic surveillance."

In other words, if you do this, we won't prosecute you. If you don't do this, we will prosecute you. And this contains items that are clearly outside of the bounds of the list that you said makes up the four corners. And that's the problem we're in because they're saying "this is what we want, you're going to do this. We're also the enforcement agency. We'll fine you \$10,000 a day unless you give us what we want."

Mr. BUYER. Well, that kind of gives good faith negotiations a bad name, sir.

Mr. WHEELER. It, it—

Mr. BUYER. I mean, I don't know how you can negotiate in good faith under that circumstance. We'll hear from the FBI and hear their position on it.

Let me share—Mr. Dempsey, you made a comment for us to please pay attention to the standard. I want you to know that I believe the members on this committee go through great pains in passing judgments when we—and there are all types of laws out there we create and we always have to do the balance test. The balance of the protection of the general welfare and protection of our citizens against individual rights and liberties and rights to privacy. We go through those pains all the time. We did it through the anti-terrorism bill and we have those inner debates among ourselves and we try to—wherever you make that cut in the decision, it becomes the target for which everyone debates and we have to pay attention which way the pendulum flows on these types of things, and especially in the telecommunications arena. We just—I don't want to get back into the debate on it, but I want you to know that we recognize that, we are cognizant of it, we appreciate you—we're going to be a good listener to you. But we also want to make sure that the FBI doesn't go beyond the scope and that the intent of Congress—

Mr. DEMPSEY. And as the technology changes, you have to constantly revisit where that balance is, because Congress can one year strike a balance and think that it has set the parameters, and then the technology moves forward. You must come forward again at that time and reassert the balance.

Mr. BUYER. Mr. Chairman, I only have one last comment. When you think about how many years it took for us to pass major legislation regarding telecommunications reform, and one of the things I remember being as a conferee on this issue is that it was such a large and momentous occasion that I couldn't help but think that—are we setting in motion subject matter that we're not going to touch for the rest of my lifetime? I don't know, because it's hard for me to envision what will the world be like in 2055? And that television will be an antiquated term, and the communications will be you'll be a walkthrough, and on your wall may be something as thin as a painting, and you just start touching it and you have instant communications and you're talking to people; you order your pizza, and you make all kinds of things, and gaining that access.

So, what I anticipate when we put this together is that whatever you come up with may be fine for today, but this dialog is a continuum. So, this relationship, for which you are saying is not pleasant, good luck, because this is a marriage here that will be difficult for a very long time. I yield back my time.

Mr. MCCOLLUM. Thank you very much, Mr. Buyer, for those poignant and salient comments.

Mr. Wexler, you are recognized for 5 minutes.

Mr. WEXLER. Thank you, Mr. Chairman. I am at a little bit of a disadvantage because I was not here when the original act was passed, and I can't identify what the intent was or wasn't. In that context, I am trying to figure out, very candidly, what the big deal is here. For anybody on the panel, it seems to me you are all uniform in suggesting that a delay needs to occur with respect to the implementation date. Assuming that the delay occurs, what is the cost to the Government for the delay?

Mr. NEEL. Well, Mr. Wexler, I would suggest that the cost could be far less. Because the path that we are now going on, if we have

to deal with a unilateral mandate to implement standards that are vastly in excess of CALEA's intent, could vastly exceed funds that have been appropriated or authorized. Thus, a delay is in order to get it right, and may actually save money or reduce the cost of CALEA.

Mr. WEXLER. Okay, but to the Government, what is the cost? Far less than what? Than not delaying, or what numbers are we talking about?

Mr. NEEL. Well, we don't yet know how much exactly it will cost to implement a final standard, because we don't have that standard. Now, on the parts that we have agreement on, there is still some dispute. Our numbers suggest somewhere between \$250 and \$600 million just for one part of it. The FBI will dispute that. So, this is an item of dispute.

Mr. WEXLER. Does anybody else—

Mr. WHEELER. I think there were, however, Mr. Wexler, some solutions outside of the standards process, and what we need to think about, if you will, are two buckets of issues. There are the buckets that are in this. There is the standard that is 100 percent compliant with CALEA, and we ought to get on with right now. And, there is another bucket of the punch list. Some of those issues can only be resolved by the courts. But, the majority of those issues can probably be resolved on a contractual basis, not a standards basis. We might consider alternative ways of getting that done, rather than trying to force them into the industry standard.

So that, if we move with this standard today, we know that it is less expensive than if we include the punch list, and so I think that what you are looking at is that if you have an extension that enables this standard to go forward, you are looking at a solution that will be less expensive in the long run than the solution that has been proposed by the FBI, which is to include these other things.

Mr. DEMPSEY. Congressman, if I may—there are two kinds of delay I think that we are talking about here. One is the unavoidable amount of delay necessary if the standard were adopted today. How long would it take? It is going to take somewhere between 18 and 24 months if it happened today. So, that is unavoidable, and has to be addressed. There is a separate type of delay, which has a cost associated with it, and that is how much longer are we going to let this go on until we reach closure?

It is our position that it is possible to take the industry standard, eliminate the location tracking provision, eliminate the packet switching provision, and start building that right now. The negotiations and the addition of other items from the punch list will only further delay.

Mr. WEXLER. Well, in the interim, in terms of wire taps is the FBI getting what it needs to get? Are there instances in which the technology is not available, and they are told no, or what's the deal?

Mr. KITCHEN. I'd like to respond to that from the PCS standpoint. We had a number of our members on the conference call yesterday, and we asked that very question. And, they said they were doing everything they can to cooperate with the FBI to provide wire taps, court-ordered wire taps, to the best of their ability. And,

while they may not be able to do all of the things, there are a number of things they have been able to do, but they are trying to comply as much as they can.

Mr. NEEL. Congressman, the wired telephone industry, which has been there for 100 years or more, predated some of these new technologies, has never refused to deliver a court-ordered wire tap. There have sometimes been technical problems that have been worked out, but we don't see a significant problem. But, I will point out one thing: In your own district, there is an historic application of wire taps of perhaps 250; it is an historic number. At any one time law enforcement may need to get in and tap about 250 lines.

What would be mandated under the FBI's capacity requirements would be the delivery, I believe, of a simultaneous wire tapping capability for those two counties of 8,793 conversations or transmissions.

Mr. WEXLER. There's only 1,000 going on nationwide all year, right?

Mr. NEEL. But here's the point, though: We are not suggesting that they would ever do that, but they would require that we be able to deliver 8,700 wire taps simultaneously. That is the problem. It is not that—we don't suspect they would ever want to wire tap everyone at the same time in that area, but that is what the standards would require us to do, and that is why we get these way out of whack projections about cost and time tables of meeting this.

Mr. MCCOLLUM. Thank you very much, Mr. Wexler. Mr. Chabot, you are recognized.

Mr. CHABOT. Thank you, Mr. Chairman. It seems that, basically, what's involved in here is somewhat of a balancing act—certainly, the balance of a legitimate law enforcement tool that is important, wire tapping, and legitimate privacy concerns, as espoused by Mr. Dempsey, and also who is to foot the bill, who is going to bear the cost of all this, and what is reasonable, and how reasonable has the FBI been in how they have handled this whole matter. And, there are, as I say, certainly, legitimate reasons to have wire tapping.

There are certain types of crime in this country that it is going to be very difficult to fight against without it: organized crime, drugs, interstate type transportation and actions that involve gambling, although I have privacy concerns. There are truly legitimate reasons to have wire tapping, but I think one of the things that makes America a great place to live is our citizenry doesn't really have to worry about when they are talking to somebody else on the phone, that the Government, or somebody else that shouldn't be listening in. Some countries can't say that.

I think we have to be very careful if we are even considering expanding the Government's ability to listen in on our conversation. So, I think many of the concerns, the privacy concerns, in particular, that Mr. Dempsey has espoused are of considerable concern to all of us, and certainly should be.

A few questions that I would like to ask: First, of Mr. Kitchen, understanding that your members are fairly new entrants into the telecommunications market, could you please explain what your particular problem is with CALEA as it is currently written, and what do you believe that we can do to ensure that the private property rights of American citizens are protected, and also that your

members would be able to compete effectively in the future, while also ensuring that law enforcement is also able to perform their necessary functions.

Mr. KITCHEN. Well, our members are unique, Mr. Cabot. As you pointed out, there are the new entrants into the market; they are the ones that are out there trying to compete. And, as Congress passed the Telecommunications Act of 1996, the whole idea was to increase competition, drive down the cost of services to the American people, and that is one of the things that the wireless industry wants to do. As new entrants, additional costs can be detrimental. Many of the new PCS entrants are small business that are just starting up, so money is very important to them. In a competitive environment they are competing with existing established carriers. The new PCS entrants are competing with Mr. Wheeler's members, the cellular carriers out there. And, we hope, in the not too distant future, they will be competing with Mr. Neel's carriers, the wire line side, to provide ubiquitous, wireless service across the country.

They are faced with a situation now under CALEA that, because they are the new entrants, and they were established after the 1995 date, they are absolutely ineligible to receive any money back from the Government for reimbursement, and there is no provision to deem them automatically in compliance, and so the January 1, 1995 cut off date is a very serious problem to them. The October 1998 date is also serious in that, as I mentioned earlier, they are out there today buying switches, putting these systems in, and they are not buying switches that are CALEA-compliant at this time, because nobody knows what that is at this point.

And, so there is nothing in the switch that guarantees that it is going to be CALEA-compliant, and if they are not CALEA compliant, they face the \$10,000-a-day fines that have been mentioned many times today. So, those two provisions in CALEA need to be changed in order for the PCS entrants to achieve a level playing field and compete in the industry as Congress proposed in the Telecommunication Act of 1996. Extending those dates, tying them to the establishment of standards, is critical to proceeding to be in a position to offer the FBI the kind of assistance that they need.

Mr. CHABOT. Mr. Neel, you had mentioned, I think, that consumers, to a considerable degree, are going to ultimately foot the bill, depending on what the price tag for this is. On the other hand, if the Government ultimately picks up some of this cost as well, we are talking about the taxpayers. And so, somebody is going to foot the bill here. I am just curious, do you have any idea—this will probably be difficult to answer real specifically—how much of the cost, if you all are footing the bill—whether it is \$1 billion or hundreds of millions, or whatever it is—how much of that percentage would actually be picked up by the consumer, as opposed to just lost profits to the company. Do you have any feel for that?

Mr. NEEL. I wouldn't even begin to speculate on that, because so much goes into this in terms of rate making. It is state commissions who really establish these rates, and how those costs would be allocated. I would point out that it is possible that consumers would not have pay a dime for this. If these negotiations are successful, and we get standards that are reasonable, technically feasible, and economically feasible, we can keep it under the \$500 mil-

lion authorized by the Congress. Then all is well, and there would not need to be any cost passed on to consumers. As far as any future costs, whether they are nominal or great, I can't speculate on how those would be allocated, because, frankly, our ratemaking process is set by State Public Service Commissions.

Mr. MCCOLLUM. Mr. Barr, you are recognized for 5 minutes.

Mr. BARR. Thank you, Mr. Chairman. I think one of my colleagues mentioned that this was a marriage. I don't think it was a marriage built of love and affection. [Laughter.]

It was really a shotgun a marriage, if anything, and certainly will want to try and avoid a divorce here, but I think a slightly more measure of fairness on the part of the Government is certainly in order at a minimum. The CALEA legislation was pushed through the—I think at literally the closing hours of the 103rd Congress, evidencing perhaps an insight on the part of the FBI that the make up of the 104th wouldn't be quite the same. I dare say that this bizarre legislation, which fundamentally alters, I think, the relationship between Government and business in law enforcement matters, in a way that does do damage to the privacy rights of both business, in terms of trade information, and citizens, is very problematic. And, I don't think the legislation would receive near a majority in the 104th or the 105th.

Notwithstanding that, Mr. Chairman, I think it is important to hold this hearing to try and make adjustments that will bring this process more back into balance. Right now it is not in balance. The Government can fine the carriers for noncompliance, even though the Government can completely determine what noncompliance is, and yet, doesn't even have to tell the carriers what compliance is. I think that the civil fine provisions, if they were looked at in a criminal setting, would be void on their face, violative of due process, vagueness, equal protection, and probably other defects.

So, I think we do have some very serious problems here, and I am glad that we are focusing in on what those problems are—hopefully, in time to prevent, I think, some very nasty events from occurring, that all of us want to avoid, and which I think would give rise to probably some legislation that would put the FBI even behind the position where it says it is now.

Mr. Wheeler, has the FBI sought switch manufactures costs, which I don't think are even shared with your carrier customers, licensing and data rights to switch manufacturers technology, audit rights, and carrier manufacturer certifications, as opposed to reimbursement to carriers for implementing such technology? In other words, are they seeking information that goes far beyond the needs and the intent of the legislation?

Mr. WHEELER. Mr. Barr, I am not privy to everything that the FBI has asked of the manufactures. What I do know is that they tried early on in the process to get data from manufacturers, and there were some disputes over that data. In the process which is underway right now, where the Department of Justice has gotten involved in the whole activity, there is a major effort to try and collect just what would it cost to do this, and how can it be done on perhaps a one-time software fix, instead of going out there and having to buy it 27,000 times for every switch in America. And,

that is the current thrust of the Department of Justice's activities is trying to collect data.

Mr. BARR. Would you say that the FBI has an incentive to delay implementation of CALEA? It would seem to increase the universe of carrier equipment of facilities installed, as opposed to deployed after January 1, 1995. Is there sort of a built-in incentive to delay?

Mr. WHEELER. Well, there seems to be a shell game going on here. I referred earlier to the Congress said go from a prop plane to a jet plane and the FBI came in and said, let's do the Apollo Program. And now we have got to pay for the Apollo Program. And, the way that is being done is you've told the FBI they only have \$500 million, and the FBI saying, "Well, how do we go and find the rest of that money to pay for all the exotic features we want? Well, one of the things they do is they hit the PCS carriers, who weren't even in existence at that point in time, as the previous question showed. The other thing is that they say that anytime that a switch is upgraded, it is immediately ineligible for reimbursement because the FBI knows that the FCC is requiring us, so that cost gets moved off onto the carrier. Let me be very clear, the document that is out there right now to upgrade our switches all the time to meet their regulatory requirements far in excess of the \$500 million that has been authorized by this committee.

Mr. BARR. I think—is the document that you were referring to earlier the ESI?

Mr. WHEELER. Yes, sir.

Mr. BARR. I think that was originally proclaimed to be a safe harbor for industry. It is in fact, though, a de facto law enforcement standard, which I think is forbidden by CALEA?

Mr. WHEELER. That was the way it was presented, Mr. Barr, and as I was reading, their language in here says, "This is what it takes to be found to a safe harbor." You will do this. If you don't do this, you won't have a safe harbor, is what the black letter of this language says in the document that they presented.

Mr. BARR. Mr. Chairman, could I just ask one very quick question of Mr. Dempsey before this panel leaves?

Mr. MCCOLLUM. Without objection, you may.

Mr. BARR. Just to clarify, I think I know the answer to this question, Mr. Dempsey, but let me just pose it very directly to you. In your view, has the FBI intervention into the industry standards-setting process gone beyond their consultative role and violated the prohibition that CALEA is precluded—the FBI is precluded in CALEA from requiring, quote—and I think this is from the statute—"any specific design of equipment, facilities, services, features, or system configurations to be adopted by any carrier or manufacturer or from prohibiting the adoption of any equipment, facilities, service, or feature by any carrier or manufacturer." Has, in your view, the FBI intervention into those industry standard-setting processes gone beyond its consultative role and violated that prohibition?

Mr. DEMPSEY. Yes, I think it clearly has, and I think that is the consensus of people here at the table, that the punch list items alone, these additional add-ons that are holding up this whole process, there is no way that you can find support for any of them in the legislation, and yet the FBI is saying, unless they are met, we

will block and continue to block this implementation and this standard, and that is clearly not what Congress intended.

Mr. BARR. Thank you.

Mr. MCCOLLUM. Thank you, Mr. Hutchinson, you are recognized for 5 minutes.

Mr. HUTCHINSON. Thank you. I want to express my appreciation to all the witnesses today, and particularly the industry for their efforts in support of law enforcement through the years. I think that should be acknowledged. I have had some experience in that arena, and my experience has been that the communications industry has really tried to aid law enforcement in carrying out their responsibilities and it certainly put a cost burden on you, and there hasn't been a whole lot of complaint. I think that the dispute today is understandable under the present set of facts. I do think this is critically important, as Mr. Dempsey has outlined, that we do more than just extend a deadline. I think it is important to give some privacy guidance from Congress on these issues, and as technology progresses that we keep privacy concerns in the forefront of that discussion. I do think, though, that there is some legitimate area of disagreement.

Mr. Dempsey, you indicated that, in reference to the punch list of ten items, that there really wasn't a basis for it in the CALEA standards. Now, I wanted you to elaborate on that a little bit, because the way I read CALEA, it is fairly broad and sets the guidelines as to what should be done, but there is certainly room for disagreement as to what should be included within those guidelines.

Mr. DEMPSEY. There is, but the question is, can you look at the punch list items and identify them with a base law enforcement capability under the four criteria in the statute, call isolation, capture of the call-identifying information to the extent that it is reasonably available, delivery of that information in a manner that allows it to be transported to a remote listening facility, and doing so in an unobtrusive manner and in a manner that protects the other communications.

I think, for example, if you look at the third-party calling feature. The FBI, in the punch list, is asking, as I understand it, for the ability to continue to monitor parties to a conference call after the target of the investigation has dropped off the call.

Mr. HUTCHINSON. I want to elaborate and talk about that a little bit more, Mr. Dempsey. In your view, is that the most offensive part of the punch list in regards to privacy concerns?

Mr. DEMPSEY. I think it probably is, because I think that there is no legal basis in the particularity clause of the Fourth Amendment, and in specification requirements of Title III, no authority for the Government to wire tap people who are not named in the order, and not using facilities specified in the order, but who were previously in communication with the target.

Mr. HUTCHINSON. Let's make sure I understand this. If my phone is subject to a title III wire tap order, and you give me a call, and I say let's bring in Mr. Flanagan, and then all of a sudden I get another call, I say you both need to hold for a minute so that I can get this other call, and then you and Mr. Flanagan can continue your conversation, the FBI wants authority to continue the tap on your conversation. Am I understanding correctly?

Mr. DEMPSEY. That's correct.

Mr. HUTCHINSON. Do they also want to have authority to continue the tap on the second call that comes in? Now, if there is a third—I don't know, can you do that on call waiting, have a third call come in?

Mr. DEMPSEY. As of now, I don't know that you can, but it may be possible. I think certainly law enforcement is entitled under the Constitution, under Title III, to monitor anybody who is in communication with the party named in the order, so that if unknown, unnamed persons call the target, and if the target then gets a third party on the line, and they are having a three-way conversation, two people previously totally unknown to law enforcement, not suspected of any involvement in crime, while they are talking to the target, the person for whom the probable cause is established, law enforcement could continue to monitor.

Mr. HUTCHINSON. But your problem is when the tap continues when the subject is off?

Mr. DEMPSEY. What happens when the target drops off.

Mr. HUTCHINSON. But, is not the wire tap on the telephone, and not directed at an individual. The tap authority from the court order is for the telephone and the conversations between you and Mr. Flanagan is still pursuant to this line and I am going to let you respond to this, but is there not a responsibility of law enforcement to minimize their listening in on a conversation not related to the criminal activity? Go ahead and respond.

Mr. DEMPSEY. On the first half, I think it is wrong to suggest that two people now having a one-on-one conversation are continuing to use the facility, the telephone, of the named target.

Mr. HUTCHINSON. If it's long distance, who is paying for it. Who is it billed to?

Mr. DEMPSEY. I am not sure that Title III should—or the Constitution, for that matter, should follow the billing practices of telephone companies. [Laughter.]

I think that certainly, if even in your hypothetical, A is the target, B calls A, B is bearing the cost of that leg of the call. If the target A then gets C on the line, and B and C keep talking, I am not sure who pays for that, but they are not using the telephone of the target. The target has now gone on to another call.

Mr. HUTCHINSON. I think your concerns are very legitimate. I think there is a great interest in the privacy aspects and we need to debate this, but are we not changing the concept of wire tap if we accept your concerns? Because the wire tap authority goes to a telephone, and if we take that away, are we not changing the whole concept of the wire tap?

Mr. DEMPSEY. Law enforcement can continue to monitor a telephone conversation of the target. So if A then calls D and has a conversation with D that can be monitored, but if you are talking about specification and particularity, I don't see how they can get authority to monitor two conversations simultaneously if the target is only on one of them.

Mr. MCCOLLUM. Thank you, Mr. Hutchinson.

I just want to clarify one thing, Mr. Neel. In response to Mr. Wexler's question, you gave some capacity information with regard to Dade County in this area, or at least some of his district.

Broward County—is it Broward County? Broward County, 8,700 calls could be monitored simultaneously, I believe you said. My understanding is that the way you calculate that, the industry does, is based upon multiplying the switches, the numbers that you can do at each switch, and the bone of contention here is the FBI is saying, hey, for every switch, we want a capacity of 200 calls, because at that point, in that part of Broward County may be where all the activity is. We may need to do 200 taps there; we may need to do zero taps in the rest of the county, but the 8,700 becomes a figure you use because you have multiplied the number of switches times the number of capacity taps at each switch. It is that right on my part?

Mr. NEEL. That's correct. I am not an engineer, but the dispute here is—or I don't know if it is a dispute—we believe that this is the capacity that they are requiring under their standard, even though we recognize that they may never use it.

Mr. MCCOLLUM. No, no, I understand, and I think this is a legitimate discussion. All I am saying is that there are some things then in the punch list that aren't very legitimate, but our purpose here today is to try and get this darn thing resolved. And, I wanted to say to everybody, and I will say it to the FBI when they get here in a minute, that that is what's in the best interest of the American people.

And, I know that there has been a discussion with the appropriators and we're the authorizers, but both of us care a lot. No one is going to be moving any dates until we get a standard. Whether that standard has to be acceptable to every party in the consensus world you have built is not as important, in my judgment, as to whether it is acceptable to us. And, while I don't want to get in the business of arbitrating the standard, I don't even want to fiddle with it—you know that is highly technical. I think in the end that would be the worst-case scenario, would be for you or somebody to come back up here and say, well, we've got the standard now, Committee, and we want all this moved.

Because, in addition to the money, Mr. Wexler, you have raised some good questions. The money, here, as I understand it, is based on retrofitting for the industry in many cases. Everything that is grandfathered is Government expense, if it is retrofitted, and that obviously there is going to have to be some retrofitting. And, you are worried now with all these changes that we are going have to put more money out, or at least the Government should put it out, instead of you, during all this delay, that we should move the grandfather date, and the Government then pays the retrofitting of all the equipment that is out there up to the date the standard is adopted.

In addition, my understanding is the Government has the obligation to pay the capacity cost, which is why the switches are so important, that we have a narrower capacity; we have less expense we're paying. This is a real dollar-and-cent issue, but it is also a practical issue. And we are here to work it out, but I think both sides have got to give a little bit. I think there may—I don't know that the numbers are right, but the FBI may have a point about the number of taps they need to make at a given switch, and we need to be sure that a reasonable amount of those taps is met, even

if the numbers appear exaggerated nationwide, or in a county.—if we realize, indeed, that it is not a question of we are going to do 1,000 taps or 8,000 taps in Broward County.

So, I am just making that point. I don't want to get into a big, extended debate. We are not here to resolve all that, just to make sure that everybody gets a feel that, while I am very sympathetic to your plight, I am also still somewhat sympathetic to The FBI. Yes, sir?

Mr. WHEELER. Mr. Chairman, one of the things we haven't discussed today that may be helpful, real quickly, is what might four corners of a solution be—and, there are, I think, four corners; there is four legs on this stool—that all these have to be resolved together in concert. One is the question of capacity, which you just raised. The other is the question of capability, which is what the standard is all about. The other is the question of cost reimbursement, and the fourth is the question of the compliance date.

We are in a situation where all of these are pulling in four different directions, and what we need to try and do, and hopefully the committee can give us all a mandate to do that, is to bring these four back, resolved as a package. But, we have got to deal with all four; we can't deal with one or two of them.

Mr. MCCOLLUM. I hear you, and I'm stimulated because I have done this. Other members wanting to say something, and I want to ask them to be very careful to restrict their time, despite my liberal comments, because we do have to go on to the next panel, in all fairness to them. Mr. Buyer did you want to get something?

Mr. BUYER. Yes, and I will make it very brief. Actually, your comments were very taken, Mr. Wheeler. You almost stole some of my thunder here, and that's fine, because you said it very, very well. You know, we make judgments here in Congress in our analysis of many different systems out there, and I couldn't help but go through my mind—and I want to do this by example, because you came out with the example of the Apollo and what the requirements and what the needs are, and what the Government ends up in their demands. You know, we set forth these requirements, and then the Government wants something really that can be classified as overreach or is it in excess.

Let me just do it here by example: The military—I sit on The National Security Committee. So we have got the C-5A out there, the C-141s which need to be replaced, and the C-130. So we need to come up with a new aircraft for our tactical and strategic airlift. So they came up with something called the C-17. And, when they set forth the requirements, and they put it in its inception, by the time we moved to production and delivery, it doubled in its price. So, we moved from about \$70 to \$140 billion, and now we find we have an aircraft you can't even—are you willing to actually take it in tactically, the threat, for fear of the loss of the cost? [Laughter.]

This is crazy. And, what happened was, when you have got so many people involved, and I'm going to say Government, the guys over at the Pentagon began this overreach. So, it's like, what is the requirement? Well, I wanted to take a jeep onto the battlefield, but what would really be nice is if I could take a Jeep Grand Cherokee onto the battlefield. That would really be great, with air-conditioning, and all kinds of CD going, and I got my car phone, too, so

I can call home and say, "Hey, Dear, everything is fine; he missed when he shot me." [Laughter.]

But I just wanted to share that as an example of the overreach and the excess of Government sometimes. So, what we find ourselves doing is reining in the excesses of Government power. And, I am sitting here stunned, and that is exactly what we have. You have got a compliance date; you have a lot of things pulling, and the question is, do we want to extend the compliance date? Right?

Mr. MCCOLLUM. Mr. Buyer.

Mr. BUYER. I understand.

Mr. MCCOLLUM. Yes, but we have got to get on to the next panel. Mr. Barr, you had a question burning?

Mr. BARR. Just one background question, Mr. Chairman, of Mr. Flanigan. I think there was some discussion earlier about the FBI stuffing the ballot box in the ANSI—or American National Standards Institute—process, and that is certainly problematic, rather than just challenging the standards of The FCC.

But, it is my understanding, Mr. Flanigan, that The FBI filed a petition with ANSI challenging your accreditation. Is that true?

Mr. FLANIGAN. That was correct, but they then lifted it after about 2 months.

Mr. BARR. Okay, but were you ever explained why they issued this challenge, this punitive action?

Mr. FLANIGAN. No, we do not know why.

Mr. BARR. They do not know why?

Mr. FLANIGAN. I did not ask them why.

Mr. BARR. Okay. Thank you. Thank you, Mr. Chairman.

Mr. MCCOLLUM. Thank you, Mr. Barr. I trust nobody else has something, I'd have to discourage you because really we have to go on.

I thank you very much for being with you today. It has been very good, and I think we have accomplished a lot. Thank you, gentlemen.

We will go on to the next panel. I would like to introduce our second panel, which consists of two members: Edward L. Allen is Chief of the Electronic Surveillance Technology Section for the Federal Bureau of Investigation. Mr. Allen joined the Bureau as a special agent in 1973, and has served in the Knoxville and New York City field offices. He was assigned to the Technical Services Division at FBI headquarters in 1982 as a Program Manager for Electronics Surveillance before being promoted to his current position. He holds a bachelor's degree from the University of Maine and a master of science and forensic science from George Washington University.

Our second witness is H. Michael Warren, Chief, CALEA Implementation Section of the FBI's Information Resources Division. His section has responsibility for implementing CALEA on behalf of the Attorney General. Mr. Warren joined The FBI as a Special Agent in 1971, and has served in the Cincinnati and Washington field offices. In 1979 he was assigned to the FBI laboratory as a forensic chemist, and was later assigned to a number of counter-intelligence-related positions. Immediately before assuming his present position he was a Special Assistant Agent in Charge of the Phoenix field office.

Mr. Allen and Mr. Warren, we welcome you both here today, and your testimony will be received. Without objection, the written testimony will be admitted to the record, and it is so ordered.

Mr. Allen, you may proceed to summarize, if you would. We probably will have to interrupt your testimony, as we have to go to vote here in a few minutes, but at least 5 minutes or so, we can give you now.

**STATEMENT OF EDWARD L. ALLEN, CHIEF, ELECTRONIC SURVEILLANCE TECHNOLOGY SECTION, FEDERAL BUREAU OF INVESTIGATION**

Mr. ALLEN. Mr. Chairman, I think what I'll do is Mr. Warren will provide our opening comments.

Mr. MCCOLLUM. Certainly, then Mr. Warren.

Mr. ALLEN. Then we'll just go on to Q&As.

Mr. MCCOLLUM. Please, Mr. Warren.

**STATEMENT OF H. MICHAEL WARREN, CHIEF, CALEA IMPLEMENTATION SECTION, FEDERAL BUREAU OF INVESTIGATION**

Mr. WARREN. Thank you, Mr. Chairman. It is a pleasure to appear before the subcommittee today to discuss the status of the Communications Assistance for Law Enforcement Act, CALEA. I am pleased to report that progress has been made, and continues to be made, since CALEA's passage 3 years ago. The progress brings law enforcement much closer today to being able to protect the personal safety of our citizens. At the same time important implementation issues remain at the forefront of our discussions. I want to assure the subcommittee that law enforcement remains committed to working with industry to implement CALEA in a timely and cost-effective manner.

Initially, we should remind ourselves of the fundamentals concerning CALEA. Both law enforcement and industry recognize that advanced telecommunications technologies had begun to systematically erode, and at times prevent law enforcement from carrying out electronic surveillance orders. This resulted in the loss of critically important evidence. Such advanced technology was having the effect of repealing de facto the legal authority established by Congress in title III and other electronic surveillance statutes.

Director Freeh and the entire law enforcement community advised the Congress that this circumstance put at great risk effective law enforcement, the public safety, and the national security; Congress agreed, and CALEA was signed into law on October 24, 1994.

The goal of CALEA was to have the industry move promptly to restore lost electronic surveillance capabilities, and to prevent new impediments from occurring. Congress established a compliance date of October 25, 1998 to convey the importance of getting this problem resolved quickly; yet, allowing industry a transition period to develop and deploy compliant solutions. To ensure the efficient and industrywide implementation, Congress encouraged the development and use of standards. While Congress expressed a preference for using the industry standards process, compliance by October 25, 1998 was required with or without standards.

Congress also recognized that there had to be equity in sharing the cost for CALEA. Therefore, Government would be responsible for modifications to equipment, facilities, and services deployed before January 1, 1995, for which Congress authorized \$500 million. The Congress also decided in CALEA that the Government should not pay carriers for modification indefinitely. After January 1, 1995, costs shift to industry.

The implementation of CALEA is in many respects a pioneering effort, involving a close cooperation of Federal, state, and local law enforcement, the telecommunications industry, and privacy groups. At a fundamental level, CALEA requires the Government, as the end user customer, to provide its requirements, although it cannot require from industry a specific design, or technological approach.

Despite the challenges of such a unique undertaking, CALEA's implementation has made important strides. A working committee has been formed that includes technical representatives from industry and law enforcement. Its purpose is to resolve the relatively few outstanding issues generated by the proposed industry standard. We have met several times, and we are very optimistic that its efforts will lead to timely implementation of the law.

Furthermore, in recent weeks we have intensified our discussions with some major manufacturers and carriers, which have yielded promising results. Several major manufacturers have recently advised the Government that they are currently developing CALEA compliant solutions, which they anticipate will be available by the October 1998 compliance date, or shortly thereafter. The Government has been informed that the solutions will meet the CALEA law enforcement requirements.

Additionally, we are only a few months away from another CALEA milestone, the final publication of law enforcement estimate of future electronic surveillance capacity. This milestone results in an unprecedented collection of intercept data, thoughtful Government analysis, and extensive consultation with the carrier community. Comments received from industry on the initial and second notices of capacity were extremely useful in enabling law enforcement to express its future interception needs.

In response to industries concerns, the final notice of capacity will make the application of these capacity numbers as clear as reasonably possible. Given this, I believe these capacity numbers will not negatively impact upon their networks, regardless of whether their approach to a CALEA technical solution is switch-based or network-based. The final notice of capacity is expected to be published in January 1998, following compliance with certain regulatory and administrative requirements.

Now, let me update you briefly on the CALEA implementation plan, submitted on March 3, 1997. As described in the implementation plan, the FBI had intended to enter into cooperative agreements with telecommunications carriers based upon reimbursement of eligible costs. However, as negotiations proceeded, it became apparent that the manufacturers' concern over competitive issues and proprietary information made it difficult for both sides to achieve their objective. Therefore, following consultation with the industry, a market-based price approach may be required for reimbursement. The Government stands ready to begin the reim-

bursement process, as soon as CALEA compliant solutions are made available, and once a reasonable market price has been determined.

In summary, law enforcement and the industry have a long history of cooperation with respect to the conduct of lawfully-authorized electronic surveillance. At its core, I believe this relationship remains a solid one, and one that allows law enforcement to bring thousands of dangerous criminals to justice each year. At the same time there is no denying the fact that dynamic changes that have occurred in telecommunications technology raise unique and complex concerns. However, I believe CALEA has held up remarkably well in providing all parties with a framework and a process to move forward. Guided by this framework, we are working diligently to bring CALEA to fruition and to meet its deadlines. We cannot, however, do it alone.

Continued cooperation is needed from all those who play a role in the implementation of this important legislation. An ongoing dialog with industry remains the cornerstone of our implementation efforts, and we look forward to continuing to work with all involved to address their concerns.

Thank you, Mr. Chairman and members of this subcommittee, for providing me the opportunity to discuss CALEA on behalf of all law enforcement. I look forward to your continued interest in the implementation of CALEA, and we are ready to answer your questions.

[The prepared statement of Mr. Warren follows:]

PREPARED STATEMENT OF H. MICHAEL WARREN, CHIEF, CALEA IMPLEMENTATION SECTION, FEDERAL BUREAU OF INVESTIGATION

Thank you Mr. Chairman:

It is a pleasure to appear before this subcommittee today to discuss the status of The Communications Assistance for Law Enforcement Act (CALEA). I am pleased to report that progress has been made and continues to be made since CALEA's passage three years ago. That progress brings law enforcement much closer today to being able to protect the personal safety of our citizens. At the same time, important implementation issues remain at the forefront of CALEA discussions. I want to assure the Subcommittee that law enforcement remains committed to working with industry to implement CALEA in a timely, cost effective manner.

Initially, we should remind ourselves of the fundamentals concerning CALEA. Both law enforcement and industry recognized that advanced telecommunications services and features had begun to systematically erode and, at times, prevent law enforcement from fully and properly carrying out electronic surveillance orders. This resulted in the loss of critically important electronic surveillance evidence. Such advanced technology was having the effect of repealing, de facto, the legal authority established by Congress in Title III and other electronic surveillance statutes. Director Freeh and the entire law enforcement community advised the Congress that this circumstance put at great risk effective law enforcement, the public safety, and the national security. Congress agreed, and CALEA was signed into law on October 24, 1994.

The goal of CALEA was to have the industry move promptly to restore lost electronic surveillance capabilities, and to prevent new impediments from occurring. Congress prudently established a compliance date of October 25, 1998, to convey the importance of getting this problem resolved quickly, yet allowing industry a transition period to develop and deploy compliant solutions. To ensure the efficient and industry-wide implementation of CALEA, Congress encouraged the development and use of standards and publicly-available technical requirements. While Congress expressed a preference for using the industry's standards process, compliance by October 25, 1998, was required *with or without standards*.

Congress also recognized that there had to be equity in sharing the costs for CALEA technical solutions. Therefore, Government would be responsible for modifications to equipment, facilities, and services deployed before January 1, 1995, a

date shortly following the passage of CALEA. In this vein, Congress authorized \$500 million to be appropriated for Government reimbursements under CALEA. The Congress also decided in CALEA that the Government should not pay carriers for modifications indefinitely. For equipment, facilities, and services deployed after January 1, 1995, the costs shift to industry. Importantly, the Congress chose not to relieve the industry of this cost responsibility in the event that a standard does not exist or is not finalized.

The implementation of CALEA is, in many respects, a pioneering effort, involving the close cooperation of Federal, State and local law enforcement, the telecommunications industry and privacy groups. At a fundamental level, CALEA requires the Government, as the end-user customer, to apprise the industry of law enforcement's requirements, although the Government cannot require from the industry a specific design or technological approach. Despite the challenges of such a unique undertaking, CALEA's implementation has made important strides and is currently focused on two major efforts: an electronic surveillance technical "capability," and interception "capacity" needs.

Law enforcement continues to work with industry on many fronts with the objective of moving forward on CALEA's capability assistance requirements. Some of these initiatives are being carried on in addition to and in parallel with a industry standard-setting process that, admittedly, has been slow and frustrating for all involved. A working committee has been formed that includes technical representatives from industry and law enforcement. Its purpose is to resolve the relatively few outstanding issues generated by the proposed standard. We have met several times and are optimistic that its efforts will lead to the timely implementation of the law.

Furthermore, in recent weeks, we have intensified our discussions with some major manufacturers and carriers, which have yielded promising results. Several major manufacturers have recently advised the Government that they are currently developing CALEA-compliant solutions, which they anticipate will be available by the October 1998 compliance date or shortly thereafter. The Government has been informed that the solutions will meet the CALEA law enforcement requirements. It is expected that other manufacturers and carriers will continue their efforts to develop timely CALEA-compliant solutions.

Additionally, we are only a few months away from another important CALEA milestone, the final publication of law enforcement's estimate of future electronic surveillance capacity. This milestone results from an unprecedented collection of intercept data, thoughtful Governmental analysis, and extensive consultation with the carrier community. The Initial and Second Notices of Capacity were extremely useful in enabling law enforcement to express its future interception needs. We believe that the core concerns raised regarding the Second Notice of Capacity are largely due to industry's misinterpretation of the way the capacity requirements would be applied to carrier networks. In response to industry concerns, the Final Notice will make the application of these capacity numbers as clear as reasonably possible. Given this, I believe these capacity numbers will then be viewed as very reasonable by carriers, and will not negatively impact upon their networks, regardless of whether their approach to a CALEA technical solution is switch or network-based. The Final Notice of Capacity is expected to be published in January of 1998, following compliance with certain regulatory and administrative requirements.

Now let me update you briefly on the CALEA Implementation Plan, submitted to each member of the Judiciary and Appropriations Committees of the House and the Senate on March 3, 1997. As described in the Implementation Plan, the FBI had intended to enter into cooperative reimbursement agreements with telecommunications carriers, based upon reimbursement of eligible "costs". However, as negotiations progressed, it became apparent that the manufacturers' concern over competitive issues and proprietary information made it difficult for both sides to achieve their objectives. Therefore, following consultation with the industry, a market-based price approach may be required for reimbursement. The Government stands ready to begin the reimbursement process as soon as CALEA-compliant solutions are made available and once a reasonable market price is determined.

In summary, law enforcement and industry have a long history of cooperation with respect to the conduct of lawfully authorized electronic surveillance. At its core, I believe this relationship remains a solid one, and one that allows law enforcement to bring thousands of dangerous criminals to justice each year. At the same time, there is no denying the fact that the dynamic changes that have occurred in telecommunications technology raise unique and complex concerns.

However, I believe CALEA has held up remarkably well in providing all parties with a framework and a process for moving forward. Guided by this framework, we are working diligently to bring CALEA to fruition, and to meet its deadlines. We can not, however, do it alone. Continued cooperation is needed from all those who

play a role in the implementation of this important legislation. An ongoing dialogue with industry remains the cornerstone of our implementation efforts, and we look forward to continuing to work with all involved to address their concerns.

Thank you Mr. Chairman, and members of this subcommittee for providing me the opportunity to discuss CALEA on behalf of all of law enforcement. I look forward to your continued interest in the implementation of CALEA and I am ready to answer your questions.

Mr. MCCOLLUM. Thank you, Mr. Warren.

We are going to take a recess, and we'll be back after this vote.  
[Recess.]

Mr. MCCOLLUM. The subcommittee will come to order. When we recessed, Mr. Warren had just finished his testimony. Mr. Allen, do you have any comments, or do you just want to go into questions?

Mr. ALLEN. No, I think we are ready for Q&As.

Mr. MCCOLLUM. Very well, happy to do that. In the other testimony that was given by the industry groups earlier today, I am sure you heard—I think you were sitting here for most of that—their concerns, and in particular, one of the things that struck me, that I have been troubled with since I heard about it, and they reiterated again today, was the suggestion that the FBI was stuffing the ballots and trying to obstruct the standards process. And, what I am curious about is, how do you answer or respond to that accusation? The statute seems pretty clear that it doesn't have a veto power for the FBI in it. What was that all about, and why was the activity performed that way, if indeed the comments that showed Sheriff Rice's response and others were prompted by The FBI? Mr. Allen?

Mr. ALLEN. Yes, Mr. Chairman. First of all, our participation in the standards process is as, if you will, a consumer or user of electronics surveillance, and what we hope we bring to that body is our experience in performing electronic surveillance. Operational criteria, we have some of the legal issues that we raise. We certainly don't bring to the table the technologists that the industry does. When the standards process first started, the document that was a genesis of that, which was an industry document, actually met our requirements. Over time that standard had been, if you will, winnowed away, and requirements had been pulled from that document that we thought were critical to our law enforcement mission.

There is, I think, some confusion on the voting process, and there still may be confusion on my part. It is still my understanding that law enforcement does not have a vote on the standard. What we did have is that we were able to submit a ballot to provide comments on the standard. In the standards process, when we attended the standards meeting, it was generally attended by a representative from The FBI, and one or more representatives from state and local or other Federal law enforcement agencies, and they represented, as they represent today, a group of about 50 law enforcement officers. They get together on a very regular basis to discuss CALEA issues, and those 50 people, in turn, represent many of the departments back in their home states.

For example, our representative from the New York Police Department, who is resident at the FBI, not only represents the New York Police Department, but the state prosecutors and some of the other state and local law enforcement agencies in New York and New Jersey as well. So, when it was time to comment on the bal-

lots, this group of 50 put together a law enforcement set of comments, and it was submitted by the FBI as our comments, and it was also submitted by those law enforcement agencies as their comments, as well.

Keep in mind that these 50 people had, in fact, been participating in the standards process through their representatives. So, we don't in any way see that as stuffing the ballots at all—the fact is that we submitted 28 ballots when we had 50 representatives representing 1000 or more law enforcement agencies.

Mr. MCCOLLUM. Apparently, Mr. Flanigan allowed that process to take place, and apparently under the rules of ANSI they are indeed votes that were binding in terms of their process, which were all obviously negative. But, in any event, I find it to be terrible that we have gotten to this point with no adoption of standards. It would be better in some ways if the industry had just gone ahead and adopted the standards, and you had fought them somewhere done the road. But, this has just delayed the process.

Now you say they've winnowed away, in the initial part, what you wanted. It that what the punch list is all about?

Mr. ALLEN. There was an initial document that came out that I believe was the start of the standards process that basically met the needs that we had under CALEA.

Mr. MCCOLLUM. Was that a document you generated, or they did?

Mr. ALLEN. No, that was an industry document.

Mr. MCCOLLUM. And that document has disappeared?

Mr. ALLEN. No, I think, as in any of these processes, there are drafts, and there are working drafts, and they change over time.

And, if I could raise another point here, there has been a lot of discussion about this ESI document that you hear of, and how that is the law enforcement standard. The ESI is a name called Electronic Surveillance Interface, and it is not our requirements for a CALEA standard; it is our recommended interface to deliver information to law enforcement. Back in 1995, law enforcement was participating in an industry-sponsored body called the Electronics Communications Service Provider Committee, and they asked law enforcement to put together a document that had law enforcement recommendations for an interface. We did prepare that document, and it is the ESI document that was referred to earlier.

Mr. MCCOLLUM. That was referred to as the standards of the FBI that you were demanding they do?

Mr. ALLEN. The standards of the FBI. And, in the first sentence of that it says that the ESI is the law enforcement recommendation for a physical interface, and it was never intended to be, and isn't to this day, a standard.

Mr. MCCOLLUM. Well, they are very insistent that you are saying, if they don't comply with that, it isn't going to work; you're not going to agree; they are going to all be held out of compliance with CALEA, et cetera, et cetera, et cetera. You don't agree with that?

Mr. ALLEN. No, that's not the case at all. A second point to raise on that is one of the members mentioned that if you didn't comply with the standard, then you wouldn't be given a safe haven under the law. When this recommendation was put forward, we were asked by industry, if we do this, would we get safe haven? It is this

one form of safe haven? And, we said, if we are putting this out as our recommendation, we would certainly have to grant you safe harbor if you comply.

Mr. MCCOLLUM. Well, let me ask you this: If the 3580 that is being voted on right now, which apparently does not have your punch list, whether that is in it, were adopted as the standard, would you challenge them in court?

Mr. ALLEN. I think the 3580, as it stands, is missing some of the functionality that we think is important for us to carry out our—

Mr. MCCOLLUM. So you would challenge them in court?

Mr. ALLEN. Yes. I think it is missing in potentially three areas. We think there is some missing functionality as it pertains to our ability to collect evidence and minimization. There is some functionality missing that goes to the integrity of the intercept: our ability to know that an intercept is, in fact, still connected, and we are not disconnected and no longer monitoring. And, there are issues that go to the cost efficiency of law enforcement being able to monitor.

Mr. MCCOLLUM. But, does the 3580 meet the standard of the act, as opposed to what you want? Does it meet CALEA's standards that are in the statute?

Mr. ALLEN. We believe, as written, it does not.

Mr. MCCOLLUM. Well, that is of course a big bone of contention. They are saying that it not only does, but they have gone far beyond what is necessary already, and that what you want is totally outside the parameters. Obviously, that is a subject that could be in great litigation, and nobody wants to see that.

Mr. Allen, my time is very limited to ask you questions today, and unfortunately, I am going to, in a minute, turn the gavel over to Mr. Barr, when I recognize Mr. Wexler, but I just want to make the observation that we don't want to move the date, but there are a lot of cost items in here. And, I haven't asked questions about that; I hope that Mr. Barr or Mr. Wexler do, but it seems to me that, no matter what we do here, eventually, when the standards are adopted—and I don't see how anything can proceed without standards; I think everybody tends to agree with that—then we are going to have to move some dates around, legislative or otherwise. It is just not practical, it doesn't seem to me, and I hope you respond to that, but I don't think it is practical to expect anybody to be able to comply with us, unless we do make those movement of those dates.

Whether we need to change anything else in the statute, I don't know. But, I am not going to suggest moving them, until you guys get together and resolve this, if there is a getting together. And, if there is not, then whenever the industry comes forward and says if that's 3580, or whatever it is, this is the standard, this is what we are going to go with; then we will consider moving dates. But, there has got to be a standard somewhere.

And, I am just very concerned that some of the capacity questions that are raised, if you are asking for too much capacity, I know you heard me talk about the switches, I know there are subtle distinctions here, but if you are asking for too much capacity, that is going to cost us. That is a taxpayer cost. Every ounce of capacity is what we are going to pay for. Now, that is more Mr. Rog-

ers' concern than mine, but it is an authorization function too. We only authorized \$500 million.

So, I again, unfortunately, am going to have to walk out of here. My time has expired, but I really, really do see you want to put on the record what your responses are to the ultimate necessity of moving a date, and the problems that we are going to be getting into as we get down the road. But, I am going to turn it over, rather than asking that response, because I have taken more time than I normally would, and I do have to be somewhere, unfortunately. I am going to recognize Mr. Wexler for his 5 minutes, and then I am going to turn the gavel over the Mr. Barr.

Mr. ALLEN. If I may just close a loop—

Mr. MCCOLLUM. Very briefly.

Mr. ALLEN. Yes, very briefly. On the punch list. As Mr. Warren mentioned, we are in discussions now with the industry, determining within that punch list which are they technically feasible to do, and what is the cost of those?

We don't know the answers to those at this point, but we think those are very essential items to get worked out, so that we can make some determination as to including those or not including those.

Mr. MCCOLLUM. Well, what Mr. Buyer said is very true. We need to reach finality on this right now, and it will never be perfect. It will never be adequate, because the technology is going to always catch up with you. Let's do the best we can, and come back to us. We will work with you, whatever we have to do, and the industry will too, I'm sure, but we have got to get this thing done.

Mr. Wexler you are recognized for 5 minutes.

Mr. WEXLER. Thank you. I would like to follow the chairman's concerns with respect to cost, and I would like to ask a couple of questions if I may. Given what you think you want, which I assume—everybody talks about this punch list—I assume you have identified "X" things that the Government wants. What is the cost of what you want? The following question is, if I understand what maybe your answer is, that you're not yet sure what the cost is. Then how can you reasonably expect the industry to be able to meet the specific deadline if the Government cannot yet determine what the cost is? If it can, please tell us what the number is.

And, then I would like to follow that by asking specifically with respect to the capacity—the capacity that the Government, as I understand it, has asked for. What is the cost associated with that? And, please share with me and the committee what the thought process or the analysis was relative to the cost-benefit of that increased capacity.

And, I appreciated very much before what I thought was the chairman's intent, was to show that while the numbers of the capacity may seem totally out of line relative to the annual amount of national need, but, in fact, on any given basis, you may need to be in a certain county with 200 of them. Could you share, in fact, how many times you have been in any county in this country where you needed 400 going at the same time, or 200 going at the same time?

Mr. WARREN. Okay, first of all, Congressman Wexler, the FBI has only recently begun to learn any estimates of cost associated

with either 3580, the industry proposed standard, or the punch list items that were omitted from the standard. We are still working with industry very closely to try to get solid information relative to these costs.

Mr. WEXLER. Would you agree with the industry that it takes 18 to 24 months to implement whatever standard is ultimately adopted?

Mr. WARREN. Yes, we would agree that that is the development time.

Mr. WEXLER. We're less than 18 months from October 1998, right?

Mr. WARREN. That is correct.

Mr. WEXLER. You don't know the cost yet, and we're less than 18 months, but yet you still don't want to extend the date. I don't get it.

Mr. WARREN. I think, two quick points if I may: First point is, as was mentioned earlier, lack of a standard does not mean that people cannot build solutions. It is done in industry all the time.

Mr. WEXLER. Okay, but if they build them now, and they haven't been approved, and then you later disapprove them, they don't get reimbursed their costs, correct?

Mr. WARREN. There has certainly been—our requirements have been known for a number of years. There has certainly been the ability for industry to come in to talk to us on proposed solutions, and would this proposed solution meet your needs, and if the answer is yes, we could implement something.

Mr. WEXLER. If they went ahead, Southern Bell in my area, Bell South, whatever it is, went ahead and built the system today, and you decided, for maybe very valid reasons, that it doesn't comply, would they or would they not be reimbursed?

Mr. WARREN. For us to do a reimbursement, or for them to go on to build a solution for the embedded base, they would enter into some sort of contractual agreement with us, and we would pay them for a certain amount of functionality. So, you would have that agreed upon upfront. So, you wouldn't have that exposure that way, yes.

I'm sorry, I interrupted you, and you were answering—

Mr. WARREN. Well, basically concerning the standard, I think it is a good point to make that the law does not require a standard be in place, and we have, since 1992, been providing the industry with law enforcement requirements relative to the needed functionality to be included in the standard, or to be built to by the manufacturers, and by the carriers.

And, we have prepared at least three documents, requirements, dated July 1992, which was done in cooperation with the industry to identify and document law enforcement's requirements. It was updated again in June 1994.

Mr. WEXLER. I appreciate that. How much is it going to cost to build what the FBI wants?

Mr. WARREN. At this point in time, we don't know what the final cost would be. We have been given estimates, just like industry has. The numbers that we are seeing are far lower than the numbers that we talked about here today. At this point in time we haven't been able to get our engineers and their engineers together

to discuss exactly how this functionality will be provided, and exactly—

Mr. WEXLER. Is there a target date when you think your engineers and their engineers could put all that together?

Mr. WARREN. We are doing it right now with some manufacturers as we speak, and we will be hopefully meeting within the next 2 months to clarify these issues relative to design capability.

Mr. WEXLER. Okay, do you think it will be before October 1998?

Mr. WARREN. You bet. I think it will be before January.

Mr. WEXLER. Okay, before January of this year?

Mr. WARREN. Yes.

Mr. WEXLER. Then they will have 9 months. And, if I could, with respect to the capability, the example was given in my particular area, 250 at the same time. How much does that cost? Have you figured all that out?

Mr. WARREN. What the capacity cost would be for doing it?

Mr. WEXLER. Well, the increased capacity. This is a dramatic increase.

Mr. WARREN. We don't know what the costs are, but I would say if we looked at the way things that are typically done today on some of the intercept solutions pre-CALEA, the cost of delivering capacity was fairly minimal compared to the cost of the solution of doing capability. And, we have typically paid for that on an ongoing basis.

Mr. WEXLER. Thank you.

Mr. BARR [presiding]. Is the gentleman from Florida finished?

Mr. WEXLER. Yes, thank you.

Mr. BARR. Mr. Warren, I think it is in your written testimony, which I think you read. Page 2, in the middle of that page, you state that "for equipment, facilities, and services deployed after January 1, 1995, the costs shift to industry." Cite for me the provision in CALEA that states that, please.

Mr. WARREN. It is in section 109 of the act: "Equipment, facilities, and services deployed on or before January 1, 1995, the Attorney General may, subject to the availability of appropriations, agree to pay telecommunication carriers for all reasonable costs directly associated with the modifications performed by carriers in connection with equipment, facilities, and services installed or deployed on or before January 1, 1995, to establish the capabilities necessary to comply with section 103"; and (b) "equipment, facilities, and services void after January 1, 1995." And, it has "determinations of reasonable achievability." Do you want me to read that?

Mr. BARR. That modifier "reasonable achievability," that would mean that such equipment is at least subject to that standard, as determined by the FCC, correct?

Mr. WARREN. That is correct.

Mr. BARR. So the cost may or may not shift to industry?

Mr. WARREN. If it is determined it is reasonably achievable, then the cost does shift to industry. If it is determined that it is not reasonably achievable, I believe, the way the legislation is written, the Government is responsible for that part that is not reasonably achievable, if they chose to do so, and if not, the equipment is considered to be in compliance.

Mr. BARR. Okay, and that is as determined by The FCC?

Mr. WARREN. That is correct.

Mr. BARR. Okay, and you agree with that, and will abide by that?

Mr. WARREN. I'm sorry, sir?

Mr. BARR. You agree with that, that that is what it says, and will abide by that?

Mr. WARREN. That it's reasonably achievable?

Mr. BARR. The FCC makes that determination, not The FBI?

Mr. WARREN. Yes, and I think there is, if you will, standards set out for determining what is reasonably achievable, and what they will consider.

Mr. BARR. On page 3 of the written testimony, in the second full paragraph, second sentence, you state, Mr. Warren, that several major manufacturers have recently advised the Government that they are currently developing CALEA compliance solutions, which they anticipate will be available by the October 1998 compliance date, or shortly thereafter. What major manufacturers have made that statement?

Mr. WARREN. Congressman, we have entered into non-disclosure agreements with those manufacturers. We will be happy to provide the names and point of contact outside the hearing, we believe.

Mr. BARR. I'd appreciate your doing that, and we certainly appreciate that in that area you do recognize that there are some limitations on information that can be disclosed. When you make a statement at the end of that sentence that the CALEA-compliant solutions would be available by October 1998, or shortly thereafter, what is the shortly thereafter? How do you read that?

Mr. WARREN. Basically, we are getting word from various manufacturers that they may have the 3580 standard available by October 1998, and they will be able to add the additional missing capabilities in a phased-in approach over the next several months or a year.

Mr. BARR. When you talk about major manufacturers, how many major manufacturers are there?

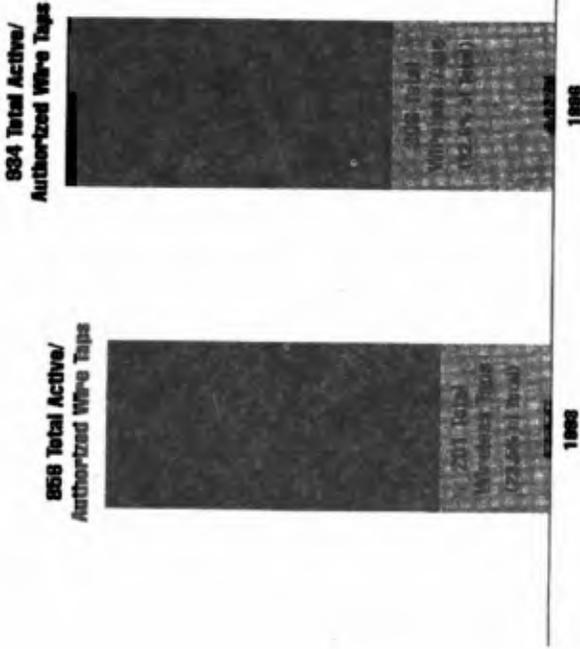
Mr. WARREN. Five or six.

Mr. BARR. Okay, and of those, how many of those five or six have recently advised you that they are currently developing CALEA-compliant solutions, which they anticipate will be available by October 1998, the compliance date, or shortly thereafter? And I understand that you will provide the specific names.

Mr. WARREN. Yes, we will.

[The information referred to follows:]

# COMPARATIVE WIRETAP STATISTICS

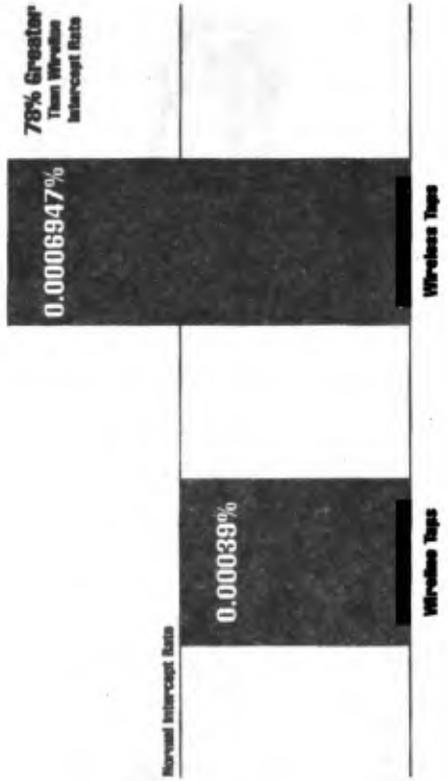


Source: 1998 and 1999 Wiretap Reports, Tables A-1 and B-1, (Administrative Office of the United States Courts).



# COMPARATIVE WIRETAP STATISTICS: 1996

[Taps as a Percentage of Total Wireline Lines vs. Total Wireless Lines]

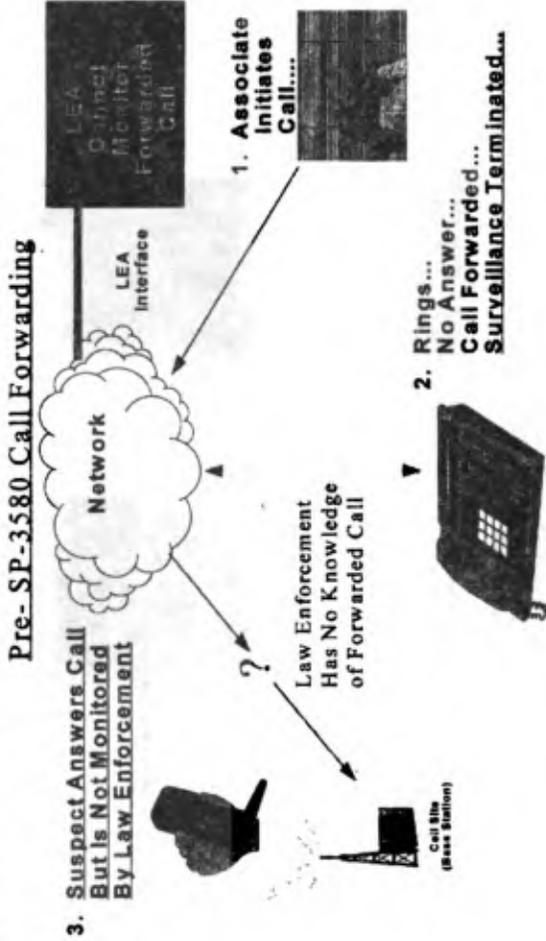


Source: 1996 Wiretap Report, Tables A-1 and B-1, Administrative Office of the United States Courts, FCC Industry Analysis Division.



### In CALEA, Congress Balanced Three Key Policies:

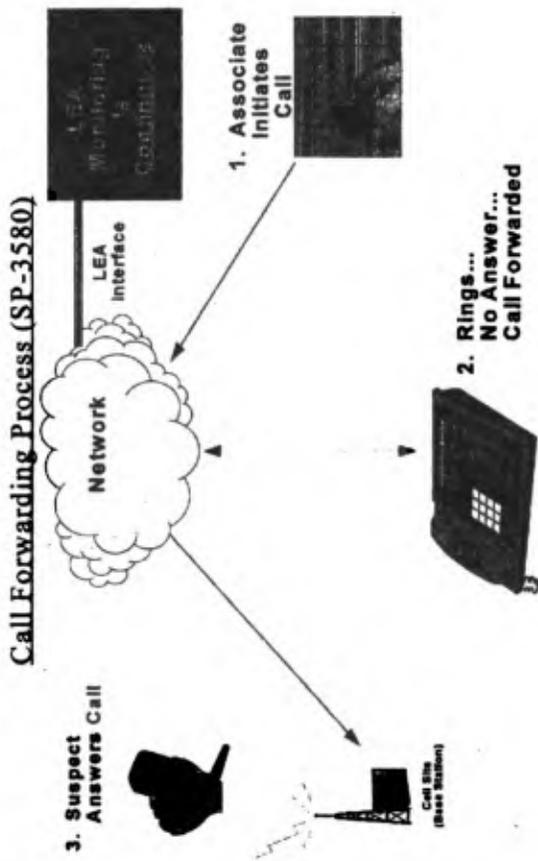
"(1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies."<sup>1</sup>



<sup>1</sup> H. Rep. No. 103-827, 103d Cong., 2d Sess. (1994) pg. 13, reprinted in 1995 U.S.C.A.N. 3489, 3493 ["House Report"].

### In CALEA, Congress Balanced Three Key Policies:

"(1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies."<sup>1</sup>



<sup>1</sup> H. Rep. No. 103-827, 103d Cong., 2d Sess. (1994) pg. 13, reprinted in 1995 U.S.C.A.N. 3489, 3493 ["House Report"].

Mr. WARREN. There are three that we are talking to right now that have given indications that they can comply.

Mr. BARR. So, of those five or six, you are saying that at least 50 percent have, in fact, recently advised you that they are currently developing CALEA-compliant solutions, which they anticipate will be available by October 1998 compliance date, or shortly thereafter?

Mr. WARREN. Yes.

Mr. BARR. Okay, and you will provide us the names of those, however many there are three or four.

Mr. WARREN. Yes, sir.

Mr. BARR. Further on page 3, the statement is made that we are only a few months away from another CALEA milestone, the final publication of law enforcement's estimate of future electronic surveillance capacity. Wasn't that required in October 1995?

Mr. WARREN. Yes, sir. We did file the first notice of capacity in October 1995.

Mr. BARR. That was a proposed?

Mr. WARREN. Yes, and based upon industry's comments, we re-evaluated the information and presented the second notice in January 1997. Again based upon industry's comments and concerns over the interpretation of that information, we have elected to file a final notice in January. We have been consulting with industry to ensure that the numbers are easily evaluated at this point, and are meaningful to their networks.

Mr. BARR. That was required under the statute by October 25, 1995, is that correct?

Mr. WARREN. It said October 25, 1995, and I think, though, there was an anticipation, that if it wasn't done by then, there was language in there that said that, once that had been filed, the carriers would have been given 3 years beyond that date. So, if it had been done by the 1995 date, then October 1998, but it had language in there that said, in effect, if that date wasn't met, then whatever date was met, it would be 3 years after that for compliance.

Mr. BARR. But the date provided in the statute was that this important CALEA milestone, which you are heralding, will be available, I guess, early next year, was required by the language of the statute to be published in October 1995. Is that correct?

Mr. WARREN. That is correct. I think when we published our first notice, we published it based on something called engineered capacity, and it received a great deal of—

Mr. BARR. I am sympathetic that when you all can't meet a deadline, there are some very good reasons for it, and you all aren't going to be fined for it, because the statute doesn't provide that. The point I am trying to make is that there are a lot of complications here, and you all have failed to meet a deadline, and that is fine. I am sure there are some very good reasons for it, but when the shoe is on the other foot, when you all make it very difficult for industry to meet deadlines, I presume that you will take the same sort of understanding attitude?

Mr. WARREN. I think we will, and I think that as far as the October 1998 date, we are prepared to look at that commensurate with industry's ability to work with us toward solutions.

Mr. BARR. Okay, now let me turn to a minute, and I think it was the chairman that touched on this, and that was that the capacity notices that we are talking about—the deadlines for the capacity notices themselves. We have some calculations here, for example, that in the Seventh Congressional District of Georgia, which is the district that I represent, just taking the single largest county in that district, which is Cobb County, which both Speaker Gingrich and I represent portions of, the number of switches in that county is 13, and the data that the FBI has provided indicates that the county historical simultaneous surveillance is 26, and that looking ahead, the county's actual simultaneous surveillance, which would be in place I think 3 years after final capacity notice, is 33, and county maximum simultaneous surveillance, which would be in place five business days following the request of the FBI, is 43. So, we would have 13 switches. The county historical simultaneous surveillance number is 26; the county actual is 33, and the county maximum is 43.

The problem becomes the prospective total requiring that the actual and maximum capacities must be available "anywhere in the county." That, I think, is what is problematic for the industry. I think that logically means to the carriers, and to me, that the carriers would be expected to provide the actual and maximum capacity numbers in each switch in the county. Otherwise, they wouldn't be available anywhere in the county, as opposed to a countywide basis, which is sort of the standard and historical basis on which these taps have been conducted in the past.

Maybe you could clarify that, because, if that is true, and I think it is a logical conclusion, because you would be requiring that the actual and maximum capacities must be available anywhere in the county, that would mean that each one of those switches, each one of those switching stations, would have to be prepared to provide for the Government the county actual simultaneous surveillance, and the maximum. And, if you then take those figures, multiplied them by—and this is just one county—by the number of switches, that is 13, you come up with astronomical figures. Instead of an actual of 33, you come up with 429, multiplying the number of switches times the county actual, and the maximum of 559. I mean, many-fold more than anybody historically would be reasonable.

And, I think that is of great concern to the industry, and I think it is probably of concern to those folks who are concerned about the numbers of taps that we are talking about here. Could you respond to that, this anywhere in the county standard, and what that really would mean, what you all have in mind, if it something other than what I have calculated?

Mr. WARREN. Congressman Barr, what that actually means is we use the actual number of 33. The carriers can distribute that capacity among all 13 switches. However, each switch has to be capable of doing at least 33. If, in fact, you were handed 33 orders and spread throughout the county, we could not hand you the 34—

Mr. BARR. Multiply 33 times 13 then?

Mr. WARREN. I am saying that the 13 switches, each switch would have to be capable of doing 33 intercepts. However, we could only ask of that county a total of 33 intercepts at any one time.

Mr. BARR. What is any one time?

Mr. WARREN. At any 1 day.

Mr. BARR. By the way, that figure is 429, when you multiply 13 times 33.

Mr. ALLEN. When we were doing the actual maximum numbers, certainly those are numbers that are necessary for somebody to plan what sort of capacity that they must be capable of having in the network, but it certainly does not preclude a carrier from initially installing one, knowing that at some point—

Mr. BARR. Wouldn't they then run afoul of the standards?

Mr. ALLEN. They could install one, and then—

Mr. BARR. I know you are trying to tell us here today that this ESI really doesn't mean anything. I don't think you all really mean that. For example, on the first page—and this was referred to earlier, I think by Mr. Wheeler—it says this ESI would satisfy law enforcement electronic surveillance needs, and would constitute an acceptable means of achieving compliance with the delivery capability requirements under section 103 of CALEA.

Now, I might agree with what you are saying earlier, in that this is simply one of perhaps a number of means. I think one can imply that, by the use of your term, would constitute an acceptable means. The problem with a lot of legal documents is the footnotes. And, the footnote, in essence, TCs—telecommunications carriers—that follow the recommendation or requirements herein for the ESI would find a safe harbor under CALEA. Well, very clearly, that indicates that if they don't do this, there would be no safe harbor. And, I think that's what gives rise also to some of the concerns you heard expressed earlier.

Mr. ALLEN. Certainly, that provision was put in there because we were specifically asked, if this was followed, would that be considered a safe harbor. So, we put the footnote at the request of—

Mr. BARR. Well, perhaps you could state right now, as official FBI policy, something that would give the industry a little bit more of a comfort level, so that this is not, in fact, held as a club over them?

Mr. ALLEN. Well, I think our intent was this is a means of achieving one of several, just as the standard, an acceptable standard will be one of many means to establish a safe harbor.

Mr. BARR. Okay. What would be some of the other ways? We are looking at one here, but what would be some of the other ways?

Mr. ALLEN. Well, for example, if a manufacturer or carrier came in and had a proposal to meet CALEA, they said we can meet CALEA. We will enter into a cooperative agreement, pay them for that, and I would assume, if I was a carrier, they would want to know that that was a safe harbor; if we do this, you pay us—will that be a safe harbor under CALEA?

Mr. BARR. Mr. Wheeler, if I could ask you, does that satisfy you? Does that give you a little more comfort level?

Mr. WHEELER. We appreciate the spirit with which it's offered. I think there is obviously concern that what Mr. Allen just said, if you come in and you persist with this, we will decide whether or not that is acceptable, and so we are back in the same Catch-22 situation where all that he has to say is, "Oh, that doesn't satisfy us."

Mr. ALLEN. I think you were asked for another means. I mean, there are probably several means. And, keep in mind too, we wouldn't enter into a cooperative to pay somebody, nor would a carrier accept that, if there wasn't some understanding that would achieve compliance under CALEA as part of a normal contractual process.

Mr. BARR. Mr. Wheeler, on this particular point, what would, you believe, to satisfy both the intent of CALEA, providing flexibility to both sides, which I think both sides need in this case, but that would give you all a comfort level that the arbitrariness would not be there so that they have absolute authority?

Okay, you need to use a microphone, perhaps the one over here to Mr. Warren's left, Mr. Wheeler, please.

Mr. WHEELER. I think, Mr. Chairman, that that is what we are trying to resolve collectively among ourselves right now, and this goes back to the four points that I was making and that Mr. Buyer responded to previously. The point is that this is a fabric, and the fabric has four main weaves in it: capability, capacity, cost reimbursement, and the compliance date. And, that we can't just solve this one problem, unless we also solve all of the others simultaneously.

I believe what I have heard Mr. Allen and Mr. Warren say, both here and in other meetings, is that they want to try to do that, and they want to and do it on those four points. I accept their good faith in that regard.

Mr. BARR. Has Mr. Wheeler correctly characterized you all's position?

Mr. ALLEN. I would characterize it a bit differently. I think what we need to do is we're trying to work through this in steps. And, the first thing we are trying to work through is to establish another safe harbor, which is this industry standard, which if people build to that, they don't need to consult with the FBI; they can build to that standard and know they are in compliance. And, that seems to be the step that we need to complete quite quickly, is to get a standard, get an agreement on what is in the standard, and allow that to be built, so that carriers can buy that solution and establish a safe haven.

I think part of the next step is capacity, and as we said, we intend to have our capacity notice—it's working its way through the rulemaking process, as we speak, and we would like to have that resolved shortly, as well.

Mr. WHEELER. I guess then what I have just heard is, no, that is not an acceptable response, that there are four weaves in this fabric, that all have to be addressed. It makes no sense to go out and write code for the capacity requirement, if you don't know what the capabilities requirement is, or vice versa, because obviously they are interrelated; they are going to build on each other. It makes no sense to write that code if the compliance date is 9 months off and impossible to meet, and it makes no sense to do that if you don't have an understanding as to which switches are covered, and if the cost be hidden under another shell. All of these go together: cost, compliance date, capability and capacity. They are inseparable.

Mr. BARR. Okay. Well, obviously, there still is a lot of work that needs to be done, and obviously, Congress is going to have to be involved in this. And we would hope—we were hoping and certainly will continue to hope—that you all will be able to work out something, but, if not, then I think we have a responsibility to try and do it. And, again, at the basis of everything we have here—and I know the FBI is in somewhat of a dilemma; the Federal Government is on this, because we want to continue to maintain a reasonable authority, reasonable capability, to intercept necessary communication for important law enforcement cases, and the technology nowadays is at such a level that nobody, back when the title III legislation was first set up, could have really envisioned.

So we need to look again at it, but we do have some concerns about basic fairness and negotiating process here. As I said, unfortunately, I was not here when CALEA was passed, not that I would have had much to do with it, but if I had, I would have configured it a little bit differently. I think it does give too much power to the Government, and I'm not sure that that really has helped the Government, either, having that power, because it creates the problems that we see here today. Perhaps if there had been a little bit more balance, you all would have been able to work a little bit more productively over the last couple of years. But it's obvious, at least at this point, that we'll have to get back involved in this.

Thank you, Mr. Wheeler. I appreciate your continuing to stick around.

If we could turn, just for a couple minutes, to some concerns—and I think we touched on these a little bit earlier, but there have been some concerns expressed, and I do share at least some of those, with regard to the authorities, the features, that seem to be beyond the scope of CALEA.

Could you all point out where CALEA mandates, for example, that law enforcement must be able to hear more than any other individual participant in a conference call?

Mr. ALLEN. If I could do that—

Mr. BARR. Or more than any other individual participant conference call is able to hear?

Mr. ALLEN. When we—

Mr. BARR. In other words, separating out the content capability—I think it's No. 11.

Mr. ALLEN. Eleven?

Mr. BARR. On this point, I think they are both economic concerns, because it would be extremely difficult—i.e., costly—to separate out the content of the conference bridge, talking about a conference call, and there are also legal questions that come into play about the admissibility of sounds that only one participant could hear, but the other participants could not. That's sort of what I'm talking about. Where does CALEA mandate that?

Mr. ALLEN. I believe that requirement would relate back to 103(a)(1), which says, "All wire and electronic communications carried by the carrier"—I'm sorry—"expeditiously isolating and enabling the Government, pursuant to court order," et cetera, "to intercept all wire and electronic communications carried by the carrier within a service area to or from equipment facilities and services

and the subscriber of such carrier concurrently with the transmission to or from the subscriber's equipment."

Mr. BARR. But isn't that "of a subscriber" of such carrier? We're talking about other people?

Mr. ALLEN. And, again, when we're talking about this and the requirement for conference calling, a couple of quick points: The first point is that we're talking about those sorts of features that are supported by the targeted service. If, in fact, you are in a conference call and it's not supported by the targeted service, then the punch list items would not apply—

Mr. BARR. What does that mean, "supported by the targeted service?"

Mr. ALLEN. For example, my service is the target of the intercept, my telephone service. You and I and Glenn are subjects of the investigation. We're subjects of the title III court order. We are talking on my service, and my service is the targeted service. I place a call to you and then I conference-in Glenn. My service, which is the targeted service, is supporting all three of our discussions.

Mr. BARR. Does the extent of the Government's authority and one's privacy rights depend on what telephone services one has?

Mr. ALLEN. The service that is the subject of the court. My service is 555-1212. It was named in the court order. Us three were named in there as participating in narcotics trafficking using my facilities. We do an intercept on my facilities. I call you, conference-in Glenn, and now we're monitoring all three.

Mr. BARR. But one of your premises was that all three of us are explicit targets?

Mr. ALLEN. Explicit are, as you are well aware, when we do court orders, we'll name the targets that we know, and the others that we haven't identified, we'll say, "others yet to be identified."

Mr. BARR. Well, what if you conferenced-in two other parties, Mr. Warren and Mr. Wheeler, neither of whom are—nobody in the Government has ever even heard of them. All of a sudden, you have these two parties involved.

Mr. ALLEN. And we're monitoring a criminal conversation?

Mr. BARR. Well, you're monitoring one of the conversations—

Mr. ALLEN. I'm monitoring our conversations where we're discussing drug trafficking—

Mr. BARR. And then you pick up a conversation between Mr. Warren and Mr. Wheeler.

Mr. ALLEN. Which is all on the same—it would all have to be on the same conference call.

Mr. BARR. Right, but the Government has never heard of them before. They're completely innocent third parties.

Mr. ALLEN. And I guess my question: They are not participating in this drug trafficking discussion?

Mr. BARR. No, they're just talking to each other.

Mr. ALLEN. Over our call? Because we're all on the same call at this point in time. We're all on the same call.

Mr. BARR. Well, with the technology, I mean, you can put people on hold and go get another call, and the Government wants the capability to monitor that conversation between Mr. Warren and Mr. Wheeler.

Mr. ALLEN. Only if it's supported by my service, only if they're conducting criminal activity that's identified in a court order, and only if they're subjects of the investigation.

Mr. BARR. But they're not.

Mr. ALLEN. So then we wouldn't be monitoring them.

Mr. BARR. But you want to have the capability to do it?

Mr. ALLEN. Right. Just as the instance when I'm monitoring myself, yourself, and Glenn, we are all parties to the criminal communication—or criminal conversations that are going on; we're all subjects of that criminal activity. And to the extent that I set my phone down at one end, the Government still has the authority to monitor the other two parties of the criminal activity that's going on over my line.

Mr. BARR. So what you're saying is, it is the position of the FBI that it can legally listen to any conversation that uses that facility or service of the intercepted target, and that that includes conversations on hold, even between parties to whom the Government never anticipated targeting, never had any information, if they are put on hold by the target's phone?

Mr. ALLEN. If they're conducting criminal activity. I mean, one has the authority to be able to monitor that—if they're not conducting criminal activity, we minimize, just as we would if you and I were talking over my service and we were not discussing criminal activity at that particular time.

Mr. BARR. Well, but we know that, certainly under the existing law and existing procedures and capabilities, we have minimization procedures that have to be followed.

Mr. ALLEN. Right, right.

Mr. BARR. But the technology you're talking about raises this to a whole new level.

Mr. ALLEN. I guess it would be—

Mr. BARR. In other words, if you're talking about a hard-line intercept, an analog intercept, this issue doesn't really even come up, because you can only hear what's on that phone—what's being discussed on the phone line. You're asking now for the capability to overhear conversations of innocent third parties who are put on hold as part of a conference call at the targeted facility?

Mr. ALLEN. As an example, we're again in our conference call; I put you on hold to answer the door; you're still conducting criminal activity supported by my service. We would want the ability to monitor that. If you're not conducting criminal activity, if you're an innocent third party sitting on my service on hold waiting for me, then we can't monitor that.

Mr. BARR. I'm not sure that everybody would feel we're comfortable with that, but I think it—without prolonging the discussion about all the legalities of that—I think the concern that a lot of people have is that these capabilities are being mandated, sought to be mandated, by the Bureau under CALEA, and I think a legitimate question can be raised that CALEA does not mandate those additional capabilities. I think that they do—that it's reasonable to consider that that is an expansion certainly of the Government's capability and wire tapping authority, too. You'd disagree; you don't see it as an expansion of the Government's wire tapping authority?

Mr. ALLEN. I would say, again, if we have identified that criminal activity, we've identified those facilities and services, we're trying to intercept, we've identified the subjects, and they're conducting criminal activity on those services, I would say we would have the authority to perform those intercepts.

Mr. BARR. I think we're going to see some fairly interesting court cases come out of all this in that case then down the road, but I think it's a problem for us that are trying to determine exactly what CALEA mandates and what it doesn't.

I apologize for not turning to the gentleman from Ohio. He's quieter than some of us, and I didn't even know he was here. The gentleman from Ohio.

Mr. CHABOT. I've been here the whole time, Bob. [Laughter.]

I appreciate the chairman's recognizing me, and I just have a few questions for the FBI here.

Mr. Warren, is it true that CALEA was intended to preserve, but not to expand law enforcement's ability to conduct criminal wire taps?

Mr. WARREN. That's correct.

Mr. CHABOT. And does law enforcement currently have the authority to track the location of a person with a cellular phone through the use of a tap—currently?

Mr. WARREN. Does it currently have the authority to track; is that what you said?

Mr. CHABOT. Right, track a person when a person uses a cellular phone under existing law?

Mr. WARREN. Yes.

Mr. CHABOT. Without CALEA?

Mr. WARREN. Yes.

Mr. CHABOT. Okay. Does the FBI seek authority—it's my understanding that Director Freeh testified back in 1994 that the FBI specifically stated that CALEA not include any location or tracking requirement.

Mr. WARREN. We have agreed with the standards bodies in the case of cellular phones that only receive information relative to the call origination and termination. No information will be tracked relative to the movement of that phone, and that's what is currently in 3580, I believe.

Mr. ALLEN. I think, too, if I may just expand on that a bit, in CALEA the definition of call identifying information is dialing or signaling information that identifies the origin, direction, or termination of each communication generated or received. There's discussion in there further on that says, pursuant to a pen register order, that such call identifying information shall not include any information that would disclose the physical location of the subscriber.

And the reason that that was included is, to the extent that call identifying information includes location information, that law enforcement couldn't receive that with a pen register order; they'd have to get a higher standing order, if you would, to receive that information.

Mr. CHABOT. How cooperative or how involved have you been in discussing with the industry the projected costs on these items? What discussions have you all had—

Mr. ALLEN. On this particular——

Mr. CHABOT. No, really in all the areas.

Mr. ALLEN. In general?

Mr. WARREN. Well, for the last several years, we have been attempting to get cost data from the industry relative to what they are proposing in the standard 3580 as well as what the additional capabilities would cost. Because they were sensitive to competitive issues and proprietary rights to that information, they chose not to—that they were either unwilling or unable to give us that information, and we've since in the last few months tried to develop other methods to identify price as a possible means of determining the cost, if you will, of the 3580 or the law enforcement requirements.

Mr. CHABOT. It's my understanding that, in response to a question by Mr. McCollum about the punch list, that you said that you are in discussions with the industry to determine technical feasibility and cost of providing the punch list. Does this mean that the FBI will insist on including those cost-effective, technologically-feasible items, even if they may be perhaps illegal because they go beyond the scope allowed under the act?

Mr. WARREN. We're currently conducting a very extensive review legally of all items requested in the punch list. With the Department, we're working very closely with the Department to evaluate each of those and its basis in title III, and the other electronic surveillance statutes. Again, we're looking at the technical feasibility and we're looking at the cost. When we have all that information available to us, we will be able to sit down with the law enforcement community and come back with a recommendation relative to whether we include or eliminate any punch list items.

Mr. CHABOT. Who within the Department is heading that up?

Mr. WARREN. The Office of Enforcement Operation, their title III people——

Mr. CHABOT. Who is that specifically?

Mr. WARREN. Fred Hess.

Mr. CHABOT. I yield back the balance of my time, Mr. Chairman. Thank you.

Mr. BARR. Thank you, Mr. Chabot.

Returning just very briefly to the last topic that we were discussing, we talked about two features, law enforcement being able to hear more than any other individual participant in the conference call can hear, law enforcement being able to wire tap not just the intercept subject's conversation, but also the conversations of other parties with whom the intercept subject is not talking, and for whom law enforcement does not have a title III order. One other concern that's been brought to our attention in terms of an additional feature is that law enforcement is to be provided with a continuous dialtone indicating whether the line carrying the wire tap from the phone company office to the police monitoring center is operating.

If those features are not provided by October 25, 1998, what will the FBI do? Will they seek punitive sanctions?

Mr. ALLEN. I think just to back up one step, the last item that you mentioned, I believe it was dialtone connected to law enforcement agencies——

Mr. BARR. Right.

Mr. ALLEN. That is something that is provided today, and basically what that does is it lets us know that we're still up on the intercepted subject. I think, as Mike mentioned, what we need to determine is we know that these are requirements that we would like to have in there; we need to see what the technical feasibility and cost—

Mr. BARR. But it's my understanding—and I'm not a technical expert on this, so I rely on what our folks here provide—the law enforcement now knows that there is a problem with the surveillance, that the is missed, and evidence is already lost. I think what we're talking about here, capability 6 and 7, is a continuity or tone check which would have told law enforcement about the problem prior to a call being placed.

Mr. ALLEN. The continuity issue is, again, the connection from the intercept point back to the law enforcement facility, and that is something today that our equipment provides, and if this intercept solution moves into a switch that's under control of the carriers, we'd expect to get a similar signal back. And, again, that provides us continuity between our equipment and the intercept. It tells us, yes, we are up, and the reason you're not getting any activity is because the subject's not using the phone.

Mr. BARR. So you're saying that the industry already provides for a continuity tone check?

Mr. ALLEN. Yes, they either provide it using their equipment that they assist us in effecting the intercept with or our equipment that we provide them to do the intercept.

Mr. BARR. Is that true, Mr. Flanigan?

Mr. ALLEN. It's called a loop extender, and it provides something called C-tone.

Mr. FLANIGAN. It's not in the present standard.

Mr. BARR. But getting back to my general question, if these various features are not provided by industry by the October 25, 1998 dead, what does the FBI intend to do?

Mr. ALLEN. Well, I think it gets back to we need to know why. If it's because it's not technically feasible or it's too costly, I think those are—

Mr. BARR. What if industry maintains its position that these are outside the scope of CALEA, and you cannot properly mandate them?

Mr. ALLEN. Well, I think that's the next part of our discussion. We're going through the technical feasibility and cost issues, and then there are legal issues that they've raised that we need to resolve. We hope to have these resolved from the technical feasibility, cost, and legal issues, so that we can agree to put into the standard what of these we can come to some commonality on.

Mr. BARR. Is, at least at this time, the Bureau's position that these features are covered by CALEA; that CALEA can properly mandate them; that they ought to be in place by October 25, 1998, and that if they're not, would there be punitive sanctions sought?

Mr. ALLEN. We would—in our discussions with OEO, Office of Enforcement Operations, they opined to us that those punch list items were allowable under CALEA; they're things that we could ask for. And, again, I think the next step is to see what the cost

and technical feasibility is of doing those. And then we can get back and discuss with the industry and OEO the legal issues again. I'm sure everybody has a legal opinion on those issues as well.

Mr. BARR. And it may be that the Congress will, pursuant to its responsibility, clarify that as well, because I don't think that—you all have been very patient—I don't think that the industry representatives, who have also been very patient in staying around for this testimony, probably feel real comfortable with this. So I think the problems, the very serious problems, are remaining, and, unfortunately, it looks as if they'll be with us and may require adjustments, legislative adjustments, to clarify the intent of CALEA.

Did you have any final questions, Mr. Chabot?

Mr. CHABOT. Yes, one final question; if the chairman, would be so kind, I'd appreciate it.

It seems from the testimony that we've heard here today that it appears to me as though the industry in general has gone through a good-faith effort to comply with CALEA's requirements, including presenting a standard for industry fairly quickly after CALEA was passed. The FBI has requested the capability to tap one out of every hundred phone conversations in its first capacity notice. It's now insisting that the industry include 10 additional capability items, and for some of them the technology doesn't even exist to comply, and I think there's some question as to whether the law even entitles them to comply. So my question would be: How strong is the FBI's commitment to come to some agreement with the industry on CALEA that's reasonable and that is in compliance with the law as it currently exists?

Mr. ALLEN. I think that, as the industry is concerned about the 10/98 date and what the implications are to them, we are certainly concerned about our continuing erosion of abilities to do electronic surveillance. Our responsibility to do that is part of the public safety. So we certainly feel that we're under tremendous pressure as well to bring this to resolution.

Mr. CHABOT. I think—I can't speak for everyone on the committee, but I certainly think that many members want to make sure that the FBI does deal in good faith with the industry, and we hope that the industry and the FBI can work this out, and that if more time is needed and is appropriate, then I think more time should certainly be considered.

So I yield back the balance of my time.

Mr. BARR. Thank you. I think the gentleman from Ohio has very capably sort of summarized where we are today. He does speak for at least this member of the committee that I don't think that we have the proper balance of power, as it were, in this equation right now, nor do I think that we have, with the very, very broad interpretations of the Bureau that we've seen here today, have a proper balance of necessary Government law enforcement authority and civil rights and privacy rights for our citizens. So I think that more questions remain unanswered than answered, and that may be the nature of this whole problem that we're trying to work through.

We have not heard the last of it. I think that we will have to take some action through the Congress, and I know you all have been, and Director Freeh has been, in touch with Chairman Rogers of the Appropriations subcommittee, as have we, and we will con-

tinue to work with them, so that we can take appropriate steps, both through the appropriations, as well as perhaps further clarifications and restrictions from a more substantive standpoint with regard to CALEA through perhaps this subcommittee, although I cannot speak for the chairman.

We appreciate the Bureau being with us today, Mr. Allen and Mr. Warren. We appreciate, certainly, the input from industry from our prior panel, and look forward to receiving the specific information, Mr. Allen, that you all will be providing us. And, of course, if any of the other panelists from either panel wish to submit any additional information in response to any specific questions or material that they think is appropriate to complete the record, and help us in our further work, we certainly will keep the record open and look forward to you all doing that.

Thank you all very much.

Mr. ALLEN. Thank you, Mr. Chairman.

Mr. BARR. This hearing is concluded.

[Whereupon, at 1:55 p.m., the subcommittee adjourned.]



LIBRARY OF CONGRESS



0 006 607 695 7

ISBN 0-16-060074-X



90000



9 780160 600746



572



572

572

572



572



572

572

572



572

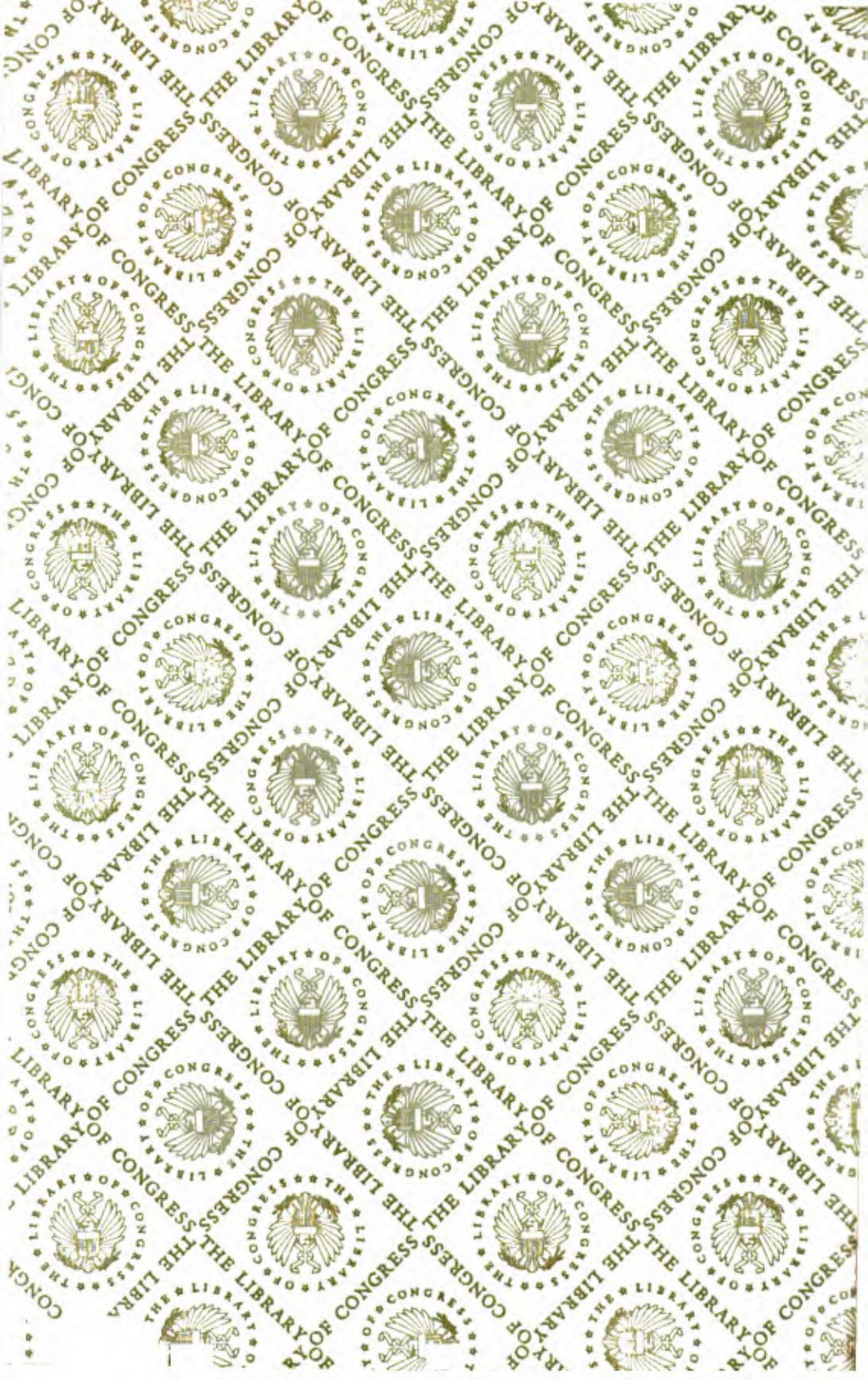
572

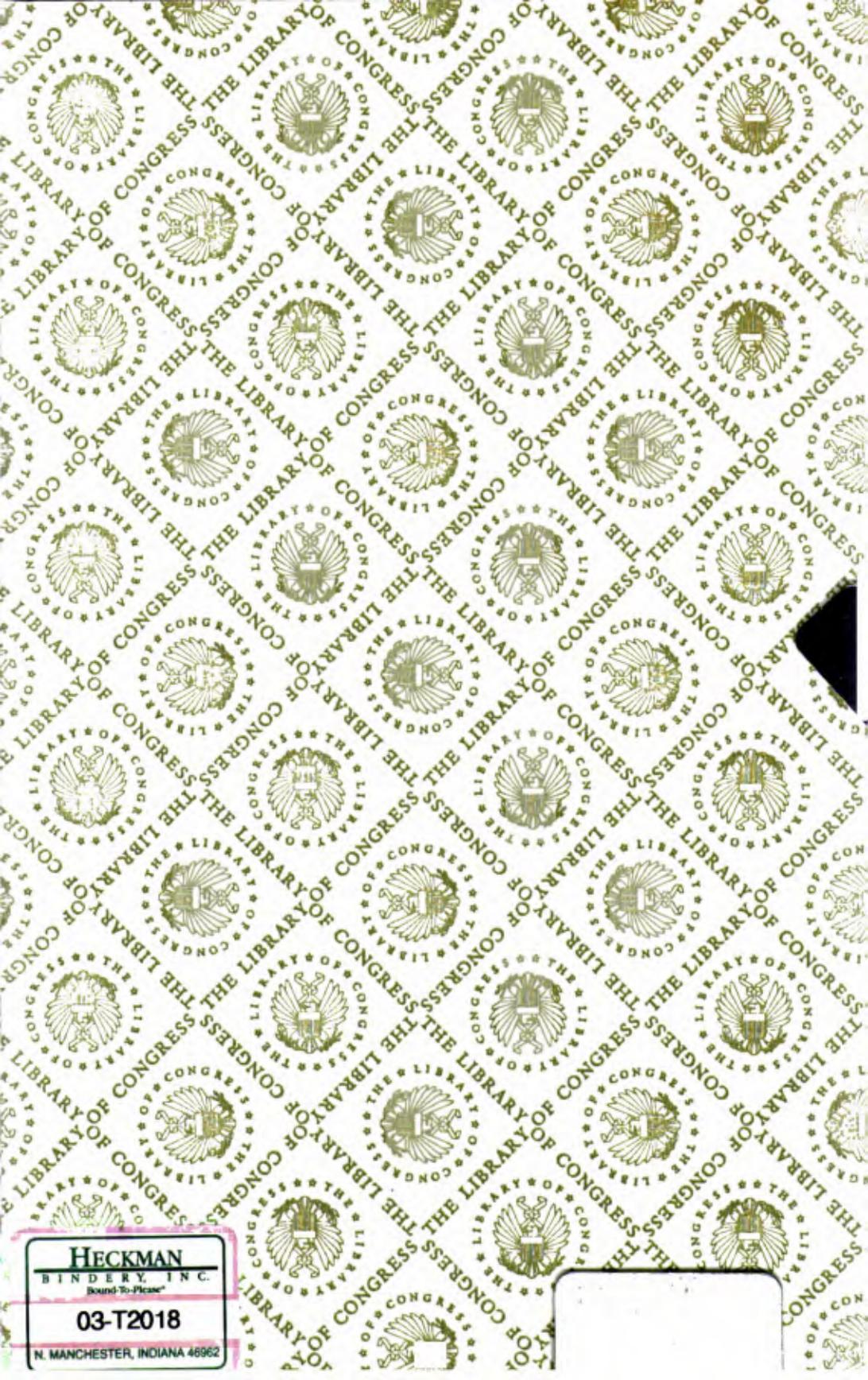


572

572

572





**HECKMAN**  
BINDERY, INC.  
Bound-To-Pleas®  
**03-T2018**  
N. MANCHESTER, INDIANA 46962

LIBRARY OF CONGRESS



0 006 607 695 7

