DOCKET FILE COPY ORIGINAL

RECEIVED

MAY 20 1998

Federal Communications Commission
Office of Secretary

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

In the Matter of	)	
	)	
Communications Assistance for Law Enforcement Act	)	CC Docket No. 97-213
	)	

To the Commission:

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER, THE ELECTRONIC FRONTIER FOUNDATION AND THE AMERICAN CIVIL LIBERTIES UNION

David L. Sobel, Esq.
Marc Rotenberg, Esq.
ELECTRONIC PRIVACY INFORMATION CENTER
666 Pennsylvania Avenue, S.E.
Suite 301
Washington, D.C. 20003

Barry Steinhardt, Esq.
President
ELECTRONIC FRONTIER FOUNDATION
1550 Bryant Street
Suite 725
San Francisco, California 94103

Steven Shapiro, Esq.
Cassidy Sehgal, Esq.
AMERICAN CIVIL LIBERTIES UNION
125 Broad Street
New York, New York 10004

Kurt A. Wimmer
Gerard J. Waldron
Alane C. Weixel
Ellen P. Goodman
Erin Egan

COVINGTON & BURLING
1201 Pennsylvania Avenue, N.W.
P.O. Box 7566
Washington, D.C. 20044-7566
202-662-6000

Attorneys for EPIC, EFF and the ACLU

Mark J. Emery
Technical Consultant
3032 Jeaninnie Anna Court
Oak Hill, Virginia 20171

May 20, 1998

No. of Copies rec'd 0+4
List ABCDE

SUMMARY

The Electronic Privacy Information Center, the Electronic Frontier Foundation and the American Civil Liberties Union urge the Commission in its implementation of the Communications Assistance for Law Enforcement Act ("CALEA") to protect the privacy rights of American citizens by finding that the interim standard adopted by industry and the "punchlist" proposed by the Federal Bureau of Investigation exceed the scope of CALEA and thus should be rejected. The Commission has a fundamental responsibility, mandated by Congress in CALEA, to protect the privacy interests of those using the Nation's telecommunications system. The Commission should protect this vital interests by commencing an independent proceeding to establish a process of public review for all matters concerning the implementation of CALEA.

Congress has recognized that the need to protect individual privacy from government intrusion, the heart of the Fourth Amendment, becomes ever more critical as the means and opportunities to invade privacy increase. Beginning with Section 605 of the Communications Act of 1934, Congress has set out clear rules protecting the privacy of communication and limiting the government's ability to surreptitiously intercept electronic communications. In 1968, Congress established a framework to allow electronic wiretapping only under the most limited circumstances. Congress made clear in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 that wiretapping was to be an investigative means of "last resort." The Electronic Communications Privacy Act in 1986 extended privacy protections to a new set of technologies such as email, cellular phones and paging devices.

Congress enacted CALEA largely in response to the FBI's concern that new technologies could be used to thwart criminal investigations. But, in attempting to accommodate the FBI's concerns, CALEA also extended privacy protections to newer technologies and required technical surveillance standards to protect privacy. The Commission has the authority -- and, indeed, the responsibility -- to ensure that privacy interests are accorded the highest priority in the implementation of CALEA. As we describe below, the role the Commission must take in protecting the public's privacy interests are quite similar to the position the Commission took in implementing the provisions of the Telecommunications Act of 1996 concerning the use of customer proprietary network information. Here, as in the CPNI proceeding, the Commission's Congressionally mandated role is, above all, to protect the privacy interests of the public.

The Commission should find that the industry's interim standard and the FBI Petition frustrate the privacy interests of federal statutes and of the Fourth Amendment. We urge the Commission to commence a proceeding that will establish appropriate standards for the implementation of CALEA in a transparent and fair manner. This proceeding – unlike the industry and law enforcement negotiations that led to the proposed "standard" – should follow Commission and Administrative Procedure Act requirements for openness and public participation; such a proceeding will result in an implementation of CALEA that is faithful to the statute's text and history.

CONTENTS

INTRODUCTION 1

I. THE COMMISSION MUST ADHERE TO THE PRIVACY PROTECTIONS AFFORDED BY THE FOURTH AMENDMENT AND CONGRESSIONAL MANDATES 5

A. The Fourth Amendment Safeguards Privacy Interests In a Manner That Should Inform The Implementation of CALEA 5

B. Congress Has Consistently and Carefully Respected Fourth Amendment Privacy Protections 6

1. Title III 6
2. ECPA 8
3. CALEA 9

II. THE COMMISSION IS OBLIGATED TO UPHOLD CALEA'S STRICT PRIVACY PROTECTIONS 11

A. CALEA Preserves And Expands Bedrock Privacy Principles 11

B. The Commission Is Obligated To Protect Privacy Interests, Much As It Has Done In Connection With Limitations on Use of CPNI 13

III. CALEA WAS NARROWLY DRAWN TO REMEDY ENUMERATED FBI COMPLAINTS, NOT TO EXTEND LAW ENFORCEMENT'S GENERAL SURVEILLANCE AUTHORITY 16

A. Congress Intended to Preserve, Not Enhance, Law Enforcement Surveillance Capabilities 16

B. The FBI Seeks to Enhance Law Enforcement Surveillance Capabilities 18

1. Location Tracking Information 19
2. Conference Calls 22
3. Packet Switching 24
4. Signaling Information 25

IV. THE COMMISSION ITSELF SHOULD ESTABLISH THE STANDARDS BY WHICH CALEA WILL BE IMPLEMENTED 28

CONCLUSION 29

RECEIVED

MAY 20 1998

Federal Communications Commission
Office of Secretary

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

In the Matter of	)	
	)	
Communications Assistance for Law Enforcement Act	)	CC Docket No. 97-213
	)	

To the Commission:

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER, THE ELECTRONIC FRONTIER FOUNDATION AND THE AMERICAN CIVIL LIBERTIES UNION

INTRODUCTION

The Electronic Privacy Information Center ("EPIC"), the Electronic Frontier Foundation ("EFF") and the American Civil Liberties Union ("ACLU") urge the Commission, pursuant to the authority established by Congress, to protect the privacy rights of American citizens in assessing whether the capabilities sought in the petition filed by the Federal Bureau of Investigation and the Department of Justice (the "FBI Petition") satisfy the requirements of the Communications Assistance for Law Enforcement Act ("CALEA") to ensure the privacy and security of electronic communications.[1] As we discuss in these Comments, the Commission has a fundamental responsibility to protect the privacy interests of those using the Nation's telecommunications system. The Commission should protect Americans' privacy interests by finding that the interim standard adopted by industry and the FBI's "punchlist" exceed the scope of CALEA and thus should be rejected. The

1 In the Matter of Communications Assistance for Law Enforcement Act, CC Docket No. 97-213, *Public Notice*, DA 98-726 (April 20, 1998).

Commission should commence an independent proceeding to establish a process of public review for all matters concerning the implementation of CALEA.

EPIC, EFF and the ACLU are the leading public interest organizations committed to protecting the privacy rights of Americans—rights that are at the core of this country's Constitutional heritage[2] and that are firmly established in the laws governing the use of the country's telecommunications system. As advancing technology increases the ability of government agents to intercept private communications, the potential threat to individual liberties grows. Advanced telecommunications dramatically multiply the number of private encounters that take place electronically. Likewise, they make government surveillance of those encounters much easier and, experience has shown, much more frequent.[3]

---

2 "Privacy is not just one possible means among others to insure some other value, but . . . it is necessarily related to ends and relations of the most fundamental sort: respect, love, friendship and trust. Privacy is not merely a good technique for furthering these fundamental relations; rather without privacy they are simply inconceivable." Fried, *Privacy*, 77 Yale L.J. 475, 477 (1968).

3 In the past 10 years, the number of interceptions per year has more than doubled. *See* Administrative Office of the U.S. Courts, 1996 *Wiretap Report for the Period January 1 through December 31, 1996* (April 1997). Reports demonstrate that:

- the use of electronic surveillance for criminal and national security investigations have increased substantially;
- court orders for electronic surveillance by state and federal agencies for criminal purposes also increased, from 1058 in 1995 to 1150 in 1996 (a nine percent increase);
- for the first time in eight years, a court denied a surveillance application;
- extensions of surveillance orders increased from 834 to 887. In all, interceptions were in effect for a total of 43,635 days in 1996.

The vast majority of interceptions continued to occur in drug-related cases: 71.4 percent (821 total) for drug investigations; 9.9 percent (114) for gambling; 9.1 percent (105) for racketeering; 3.5 percent (41) for homicide and assault and a few each for bribery, kidnapping, larceny and theft, and loansharking. No orders were issued for "arson, explosives, and weapons" investigations. This increased quantity of electronic surveillance is, moreover, relatively inefficient. Overall, 2.2 million conversations were captured in 1996. Prosecutors deemed a total of 1.7 million intercepted conversations not "incriminating". Each interception resulted in the capture of an average of 1,969 conversations. Prosecutors reported that on average, 422 (21.4 percent) of the conversations were

Congress traditionally has recognized that the need to protect individual privacy from government intrusion, the heart of the Fourth Amendment, becomes ever more critical as the means and opportunities to invade privacy increase.[4] Beginning with Section 605 of the Communications Act of 1934, Congress has set out clear rules protecting the privacy of communication and limiting the government's ability to surreptitiously intercept electronic communications.[5] In 1968, Congress established a framework to allow electronic wiretapping only under the most limited circumstances. Congress made clear in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III") that wiretapping was to be an investigative means of "last resort."[6] The Electronic Communications Privacy Act

---

"incriminating." Federal intercepts were particularly inefficient, with only 15.6 percent of the intercepted conversations reported as "incriminating."

4 H. R. Rep. No. 99-647 at 18 (1986) ("Today, we have large-scale electronic mail operations, cellular and cordless telephones, paging devices, miniaturized transmitters for radio surveillance, and a dazzling array of digitized information networks which were little more than concepts two decades ago. Unfortunately, the same technologies that hold such promise for the future also enhance the risk that our communications will be intercepted by either private parties or the government.").

5 *See* 47 U.S.C. § 705 ("No person not being authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect or meaning of such intercepted communication to any person").

6 *See generally* E. Lapidus, EAVESDROPPING ON TRIAL (1974). Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act, Pub. L. No. 90-351. tit. III, 82 Stat. 212 (codified as amended at 18 U.S.C. §§ 2510-2522 (1996)), in part to protect the privacy of communication from the abuse of electronic surveillance techniques made possible by technological advances:

> The tremendous scientific and technological developments that have taken place in the last century have made possible today the widespread use and abuse of electronic surveillance techniques. As a result of these developments, privacy of communication is seriously jeopardized by these techniques of surveillance.

Senate Committee on the Judiciary, Omnibus Crime Control and Safe Streets Act of 1967, S. Rep. No. 90-1097, at 67 (1968).

in 1986 ("ECPA") extended privacy protections to a new set of technologies such as email, cellular phones and paging devices.[7]

Congress enacted CALEA largely in response to the FBI's concern that new technologies could be used to thwart criminal investigations. But, in attempting to accommodate the FBI's concerns, CALEA also extended privacy protections to newer technologies and required technical surveillance standards to protect privacy. The Commission has the authority and, indeed, the responsibility to ensure that privacy interests are accorded the highest priority in the implementation of CALEA.[8] As we describe below, the role the Commission must take in protecting the public's privacy interests are quite similar to the position the Commission took in implementing the provisions of the Telecommunications Act of 1996 concerning the use of customer proprietary network information.[9] Here, as in the CPNI proceeding, the Commission's Congressionally mandated role is, above all, to protect the privacy interests of the public.

Groups dedicated to the protection of privacy expressed grave reservations in 1994 about the potential for CALEA to be used improperly by law enforcement to expand the scope of electronic surveillance; with the filing of the FBI Petition, these concerns have been realized. The Commission should find that the industry's interim standard and the FBI Petition, if granted, would frustrate the privacy interests of federal statutes and of the Fourth

---

7 Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. §§ 2510-2521, 2701-2710, 3121-3126) (hereinafter "ECPA").

8 47 U.S.C. § 1006.

9 *See* Implementation of the Telecommunications act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, CC Docket No. 96-115, *Second Report and Order and Further Notice of Proposed Rulemaking*, FCC 98-27,

Amendment. The FBI seeks surveillance capabilities that far exceed the capabilities the FBI has had in the past and is entitled to under the law. For these reasons, we urge the Commission to reject the interim standard and the FBI Petition and commence a proceeding that will establish appropriate standards for the implementation of CALEA in a transparent and fair manner. This proceeding – unlike the industry and law enforcement negotiations that led to the proposed "standard" – should follow Commission and Administrative Procedure Act requirements for openness and public participation; such a proceeding will result in an implementation of CALEA that is faithful to the statute's text and history.

I. THE COMMISSION MUST ADHERE TO THE PRIVACY PROTECTIONS AFFORDED BY THE FOURTH AMENDMENT AND CONGRESSIONAL MANDATES.

A. The Fourth Amendment Safeguards Privacy Interests In a Manner That Should Guide The Implementation of CALEA.

In 1967, the Supreme Court ruled that subjects of electronic surveillance were protected by the Fourth Amendment's restrictions on searches and seizure. In *Berger v. New York*, the Court held that lengthy, continuous or indiscriminate electronic surveillance violated the Fourth Amendment.[10] Likewise, *Katz v. United States* held that electronic surveillance was constitutionally permissible if it were short, directed to intercept only a few conversations, approved in advance by a judge, and supported by a special showing of need.[11] These holdings provide the underpinnings for both Title III and the Commission's implementation of CALEA. Both Congress and the Commission must be faithful to

---

para. 2 (February 26, 1998).

10 388 U.S. 41 (1967).

11 389 U.S. 347 (1967).

constitutional and statutory limitations on the government's ability to design systems to facilitate electronic surveillance.

B. Congress Consistently and Carefully Has Respected Fourth Amendment Privacy Protections.

Responding to *Berger* and *Katz*, Congress decided to institutionalize in federal statutes the Fourth Amendment privacy protections to which law enforcement must adhere.

1. Title III

Title III, enacted a year after *Berger* and *Katz*, was Congress's response in the form of national legislation to a body of law "totally unsatisfactory in its consequences" for privacy and justice.[12] Title III had two purposes: (1) protecting the privacy of wire and oral communications and (2) providing a uniform basis for authorizing law enforcement personnel to intercept those communications.[13] "The restraint with which [limited authority for wire tapping] was created reflects the legitimate fears with which a free society entertains the use of electronic surveillance."[14]

Title III devoted special attention to individual privacy concerns, in part because electronic surveillance poses greater threats to privacy than do the physical searches and seizures that inspired the Fourth Amendment. Electronic surveillance tends to be indiscriminate, catching communications that may or may not even be relevant to an investigation much less contemplated by a court order. Electronic surveillance also tends to extend for long stretches of time. And it is conducted surreptitiously and without notice to

---

12 S. Rep. No. 90-1097 at 69 (1968).

13 *Id.* at 66.

14 *United States v. Kalustian*, 529 F.2d 585, 588 (9th Cir. 1976).

the subject or to other persons participating in electronic communications. All of these features distinguish it from searches and seizures that must be particular and conducted with "knock and notice."[15] To mitigate some of the more dangerous characteristics of electronic surveillance, among other things, Title III requires that government surveillance minimize the interception of innocent conversations.[16]

Title III's privacy safeguards in the form of particularity and minimization requirements are derived directly from *Berger*. Because eavesdropping is a broad intrusion on privacy, "[t]he need for particularity and evidence of reliability in the showing required when judicial authorization of a search is sought is especially great in the case of eavesdropping."[17] The *Berger* Court found that New York's eavesdropping statute was a "blanket grant of permission . . . without adequate judicial supervision or protective procedures."[18] Despite the state's contention that eavesdropping was a crucially important investigative technique, the Court refused to diminish the importance of the Fourth Amendment for the sake of law enforcement.[19] "Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices."[20] Taken as a whole, Title III established an elaborate framework to minimize the government's use of wiretapping as an investigative technique and to ensure accountability in the execution of this authority.

---

15 *See Richards v. Wisconsin,* 117 S. Ct. 1416 (1997).

16 18 U.C.S. § 2518(5). In addition, surveillance must be, *inter alia,* for limited periods of time, for specified crimes, and only as a last resort. *See* 18 U.S.C. § 2518 (3).

17 *Berger v. New York*, 388 U.S. 41, 56 (1967).

18 *Id.* at 59.

19 *Id.* at 62 ("[W]e cannot forgive the requirements of the Fourth Amendment in the name of law enforcement.").

2. ECPA

In the 1980s, Congress determined that legal protection of privacy had not kept pace with technology: "[T]he law must advance with the technology to ensure the continued vitality of the fourth amendment."[21] Congress concluded that without statutory protection for rapidly expanding wireless and digital communication technologies, such as e-mail, citizens faced the erosion of their "precious right" of privacy.[22] Accordingly, in 1986, Congress enacted Electronic Communications Privacy Act of 1986 ("ECPA").

ECPA updated Title III by prohibiting interception and disclosure of "electronic communications" as well as wire and oral communications.[23] In addition to expanding privacy protection to content carried by new communication technologies, ECPA extended some privacy protection to transactional information generated by communications systems. ECPA required a court order for pen registers, which identify the numbers of outgoing calls, and for trap and trace devices, which identify the numbers of incoming calls.[24] In addition, ECPA prescribed rules that limited law enforcement access to information identifying subscribers of electronic communications services.[25]

---

20 *Berger,* 388 U.S. at 63.

21 S. Rep. No. 99-541 at 5 (1986).

22 *Id.*

23 18 U.S.C. § 2511(1).

24 18 U.S.C. §§ 3121-3122.

25 18 U.S.C. § 2703.

3. CALEA

Congress enacted CALEA in response to technological developments that, according to an "informal survey" prepared by the FBI that it refused to release to the public,[26] impeded law enforcement's electronic surveillance capabilities.[27] But, as the FBI recognizes, CALEA was not designed to increase law enforcement surveillance capabilities nor otherwise to undermine the privacy protections that make statutory surveillance constitutional. As discussed below, CALEA, reaffirming Title III, requires law enforcement to minimize intrusion on irrelevant conversations.[28] As the Supreme Court has recognized, minimizing intrusion into communications is central to the constitutionality of wiretaps.[29] Indeed, unless government surveillance minimizes the catch of communications, it does not satisfy the particularity requirements of the Fourth Amendment.[30] CALEA did not change the direction of federal protection of privacy interests and limitations on law-enforcement surveillance activities; rather, it continued on the same course of seeking to meet the limited and targeted

---

26 *See Electronic Privacy Information Center v. Federal Bureau of Investigation*, 865 F. Supp. 1 (D.D.C. 1994) ("In lobbying for the new wiretapping law, the FBI chose to only release a summary" of the survey).

27 *See* Testimony of Louis J. Freeh, Director, Federal Bureau of Investigation, Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearings on H.R. 4922 and S. 2374, Before the Subcommittee on Technology and the Law, the Senate Committee on the Judiciary, the Subcommittee on Civil and Constitutional Rights, and the House Committee on the Judiciary, 103rd Cong. 6 (1994) (hereinafter "CALEA Hearings").

28 *See* Section 103(a)(4).

29 *See Berger v. New York*, 388 U.S. 41, 63 (finding that a warrant or statute can be drawn to meet Fourth Amendment requirements when eavesdropping is permitted in only "the most precise and discriminate circumstances.").

30 *See id.*. at 55 (The Fourth Amendment commands that a warrant issue not only upon probable cause supported by oath or affirmation, but also "particularity describing the place to be searched and the persons or things to be seized.").

needs of law enforcement while accomplishing the overriding need to protect the constitutional rights of the American public.

Like ECPA, CALEA deals with the confrontation between new technology and established privacy interests. Courts often have been called on to address traditional privacy and Fourth Amendment issues in connection with new technologies. For example, in *Brown v. Waddell*,[31] the Fourth Circuit held that a digital display pager clone was not a pen register within the meaning of ECPA.[32] Thus, according to the court, pager clone interception of numeric messages intended for the suspect's digital display pager was an unauthorized interception of electronic communications pursuant to 18 U.S.C. § 2511.[33] In a similar effort to protect privacy interests, the court in *In re Application of U.S. for Order Authorizing Use of Cellular Telephone Digital Analyzer*,[34] analyzed a federal prosecutor's proposed order for using the digital analyzer under the statutes governing the use of pen registers and trap and trace devices.[35] The court concluded that the proposed order was deficient because it did not limit the digital analyzer's use to the court's jurisdiction.[36] And, to the extent that a digital analyzer is analogous to a pen register, the court determined that the order did not ensure the accountability that the statute demands for the use of a pen register.[37]

---

31 50 F.3d 285 (4th Cir. 1995).

32 *Id.* at 294.

33 *Id.*

34 885 F. Supp. 197 (C.D. Cal. 1995).

35 *Id.* at 200-01.

36 Section 3123(b) requires that an order state the number and, if known, the physical location of the telephone line to which the pen register or trap and trace device is to be attached. 18 U.S.C. § 3123(b)(1)(C).

37 885 F. Supp. at 201.

The Commission should, as Congress has, provide privacy protections that withstand the evolution of new technology and, as many courts have, construe law enforcement's surveillance authority narrowly with respect to new technologies. The Commission should ensure that its rules implementing CALEA minimize intrusion on individual privacy and do not permit law-enforcement interests to overwhelm the privacy interests that also must be weighed heavily in the balance.

II. THE COMMISSION IS OBLIGATED TO UPHOLD CALEA'S STRICT PRIVACY PROTECTIONS.

CALEA continues the tradition of enforcing privacy rights in the face of technological innovation and development. Adhering to the values embodied in the Fourth Amendment, CALEA seeks to protect the American public's communications privacy to the greatest extent possible while, at the same time, to provide for legitimate law enforcement needs. The Commission is obligated to follow the balance that Congress sought to strike between these twin goals.

A. CALEA Preserves And Expands Bedrock Privacy Principles.

In adopting CALEA, Congress sought to further three interests: the legitimate surveillance needs of law enforcement; the American public's right to privacy and the desire to foster technological innovation.[38] To balance these objectives, Congress imposed several limitations on the ability of law enforcement to intercept communications and expanded the privacy protections inherent in the ECPA.

---

38 H.R. Rep. No. 103-827, pt. 1, at 13 (1994) ("Therefore, the bill seeks 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

CALEA imposes four requirements on the telecommunications industry. Three of the requirements are intended to preserve law enforcement's surveillance capabilities and the fourth, equally important, is intended to uphold the privacy interests of the American public. Specifically, carriers must ensure that their facilities are capable of: (1) expeditiously isolating and enabling law enforcement to intercept call content; (2) expeditiously isolating and enabling the government to access reasonably available "call-identifying information;" (3) delivering intercepted communications and call-identifying information to the government in a format that allows them to be transmitted to a law enforcement listening facility; and (4) doing all of the above three functions "in a manner that protects ... the privacy and security of communications and call-identifying information not authorized to be intercepted" and the confidentiality of the interception. *See* 47 U.S.C. 1002(a)(1)-(4).

CALEA thus requires telecommunications carriers to safeguard the privacy of communications and call-identifying data not authorized to be intercepted. In a further effort to protect privacy interests, CALEA prohibits law enforcement from using pen register devices for tracking purposes,[39] and improves the privacy of mobile phone communications.[40] The statute also expands the privacy protections of the ECPA in the area of cordless telephones and certain radio-based telecommunications.[41]

---

communications services and technologies.").

39 *See* 47 U.S.C. § 1002(a)(2).

40 *See* Public Law No. 103-414, § 206 (expanding criminal penalties for stealing service from legitimate users).

41 *See* Public Law No. 103-414, §§ 202, 203; *See* H.R. Rep. No. 103-827, at 10 ("S. 2375 also expands privacy and security protection for telephone and computer communications.").

Most importantly, as the legislative history establishes, CALEA advances privacy protections by limiting the surveillance capabilities of law enforcement.[42] Congress recognized that "as the potential intrusiveness of technology increases, it is necessary to ensure that government surveillance authority is clearly defined and appropriately limited."[43]

B. The Commission Is Obligated To Protect Privacy Interests, Much As It Has Done In Connection With Limitations on Use of CPNI.

Congress could have placed full responsibility for implementation of CALEA squarely on the shoulders of the Department of Justice or the FBI. It chose not to do so. Its choice was to place an independent regulatory agency at the intersection of law enforcement and industry positions – not only to mediate between these groups but also to protect the privacy interests of the American public. As the structure and history of CALEA clearly provide, Congress intended the Commission to review the adequacy of the technical standards developed pursuant to CALEA and ensure that privacy interests of Americans would be protected. Section 107(b), entitled Commission Authority, states:

> If industry associations or standard-setting organizations fail to issue technical requirements or standards or if Government agency or any other person believes that such requirements or standards are deficient, the agency or person may petition the Commission to establish, by rule, technical or requirements or standards that . . . (2) protect the privacy and security of communications not authorized to be intercepted.[44]

---

42 *See* H.R. Rep. No. 103-827, at 18 ("It is also important, from a privacy standpoint, to recognize that the scope of the legislation has been greatly narrowed."); *id.*, at 22 ("The committee intends the assistance requirements in [CALEA] to be both a floor and a ceiling."); *id.*, at 23 ("The committee urges against overbroad interpretation of the requirements. . . . The committee expects industry, law enforcement and the FCC to narrowly interpret the requirements.").

43 H.R. Rep. No. 103-827, at 17.

44 47 U.S.C. § 1006.

The Commission's role was an integral part of the structure that Congress intended to create in enacting CALEA. The report from the House Judiciary Committee states:

> H.R. 4922 includes provisions, which the FBI Director Freeh supported in his testimony, that add protections to the exercise of the government's current surveillance authority. Specifically, the bill -- . . . 4. Allows any person, including public interest groups, to petition the FCC for review of standards implementing wiretap capability requirements, and provides that one factor for judging those standards is whether they protect the privacy of communications not authorized to be intercepted.[45]

Similarly, Section 109 of CALEA directs the Commission to address privacy issues that may arise when implementing the statute's terms:

> The Commission, on petition from a telecommunications carrier or any other interested person, and after notice to the Attorney General, shall determine whether compliance with the assistance capability requirements of section 103 is reasonably achievable with respect to any equipment, facility or service installed or deployed after January 1, 1995. . . . In making such determination, the Commission shall . . . consider the following factors: . . . The need to protect the privacy and security of communications not authorized to be intercepted.[46]

In adopting CALEA, Congress recognized the dangers to privacy interests inherent in its mandate to facilitate limited electronic surveillance. To ensure that the needs of law enforcement are appropriately balanced against the values of privacy, Congress authorized the Commission to regulate the ways in which the nation's telecommunications systems can assist the government in preserving the privacy needs of the American public and the surveillance needs of law enforcement. And indeed, this proceeding before the Commission

---

45 H.R. Rep. No. 103-827 at 17-18.

46 47 U.S.C. 1008(b)(1).

is the first time during the implementation of CALEA that privacy interests have been fully represented.

The role given to the Commission under CALEA as the guardian of privacy interests in not a new role for the Commission. The Commission has often found itself as the referee in conflicts involving consumer privacy concerns. One of the most recent of such conflicts involved telecommunications carriers' use of customer proprietary network information ("CPNI"). CPNI includes information that is extremely personal to telecommunications customers, such as to whom, where, and when a customer places a call, as well as to which telecommunications services a customer subscribes and the extent to which those services are used.[47] This information is also commercially valuable to telecommunications carriers.

In the Telecommunications Act of 1996 (the "1996 Act"), Congress established a new framework which balances customer privacy interests with carriers' interests in utilizing CPNI for marketing purposes.[48] In adopting regulations implementing the CPNI privacy provisions, the Commission's goal was to clarify the balance established by Congress. The Commission further found that states could not adopt regulations inconsistent with the Commission's CPNI implementing regulations. The Commission concluded that Congress sought to strike an appropriate balance between customer privacy interests and carriers' interests in utilizing CPNI. State regulations that expand carriers' abilities to use CPNI

---

47 Implementation of the Telecommunications act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, CC Docket No. 96-115, *Second Report and Order and Further Notice of Proposed Rulemaking*, FCC 98-27, para. 2 (February 26, 1998) ("*CPNI Order*").

48 The Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996), codified at 47 U.S.C. § 222.

would upset Congress' balance and accordingly must be preempted (just as state restrictions that place greater burdens on carriers must be preempted as well).[49] A similar respect for the balance struck by Congress is appropriate here.

III. CALEA WAS NARROWLY DRAWN TO REMEDY ENUMERATED FBI COMPLAINTS, NOT TO EXTEND LAW ENFORCEMENT'S GENERAL SURVEILLANCE AUTHORITY.

A. Congress Intended to Preserve, Not Enhance, Law Enforcement Surveillance Capabilities.

In adopting CALEA, Congress emphasized that the statute's capability assistance requirements would serve as "both a floor and a ceiling" on government surveillance demands.[50] Congress acted to protect privacy interests by refusing to permit the FBI the authority it sought over the implementation of CALEA, by delegating implementation authority to the Commission, and by enacting explicit privacy protections. To guarantee that surveillance is not expanded, CALEA requires telecommunications carriers to protect user privacy and security of information they are not authorized to intercept. Further, Congress directed industry, law enforcement and the Commission "to narrowly interpret" the requirements of CALEA.[51]

Congress made clear that CALEA was not intended to provide new surveillance capabilities but to maintain the ability of law enforcement to gain access to information permitted in the analog world under Title III. Indeed, the FBI agreed with this goal during the legislative process. During the hearings which lead to the enactment of CALEA, the FBI

---

49 *CPNI Order*, para. 18.

50 H. R. Rep. No. 103-827 at 22.

testified that it "was not seeking any expansion of the authority Congress gave to law enforcement when the wiretapping law was enacted. . . ."[52] In its Petition, the FBI acknowledged that CALEA was designed "'to preserve the status quo.'"[53] Indeed, the sole evidence Congress had before it when it enacted CALEA was an FBI "informal survey" of some "183 instances" in which electronic surveillance allegedly was frustrated by new technology. These "instances" do not mirror the expanded capabilities the FBI now is seeking in its Petition – of the 183 examples, 54 dealt with cellular port capacity; 33 dealt with inability to capture dialed digits contemporaneously with audio; 20 dealt with speed dialing, voice dialing or call waiting; 10 dealt with call forwarding; 12 dealt with voice mail; and 42 dealt with various technologies such as call-back.[54]

Thus, there is no disagreement that CALEA was designed to preserve the existing statutory and constitutional accommodation between law enforcement's surveillance needs and privacy interests.[55] CALEA "was intended to provide law enforcement no more and no

---

51 *Id.* at 23.

52 CALEA Hearings, Testimony of Director Freeh, at 6. *See also* CALEA Hearings, Testimony of Director Freeh, at 10 ("We are not asking [Congress] to expand the authority that we have to do wiretapping."); at 16 ("The proposed legislation explicitly states that the legislation does not enlarge or reduce the government's authority to lawfully conduct court-ordered electronic surveillance and install or use court-ordered pen register or trap and trace devices."); and at 29 ("[T]he proposed legislation does not seek to expand the current laws authorizing the interception of wire or electronic communications. To the contrary, this proposal simply seeks to maintain law enforcement's ability to conduct the types of surveillance currently authorized [under wiretap laws].").

53 FBI Petition at 16 (quoting H.R. Rep. 103-827, at 22).

54 H.R. Rep. 103-827 at 22.

55 "Some may claim that without the use of [eavesdropping] devices crime detection in certain areas may suffer some delays since eavesdropping is quicker, easier and more certain. However, techniques and practices may well be developed that will operate just as speedily and certainly and –

less access to information than it had in the past."[56] Accordingly, CALEA may not be used by the FBI to expand law enforcement's surveillance capabilities.

B. The FBI Seeks to Enhance Law Enforcement Surveillance Capabilities.

Through its participation in the industry standard-setting procedure and now this proceeding, the FBI has attempted to use CALEA to expand law enforcement surveillance capabilities. In a surprising turnabout from its position before Congress, the FBI Petition now claims that CALEA authorizes it to expanded surveillance capacities:

> Section 103 does not restrict this obligation to the communications and call-identifying information that were accessible in the pre-digital era. More generally, the language and legislative history of CALEA make clear that Congress intended for the electronic surveillance capabilities of law enforcement to keep pace with technological developments in the telecommunications industry. As technological changes have made possible new communications services, new information is generated regarding the use of such services by subscribers. Law enforcement cannot preserve the status quo in a meaningful sense unless it is able to obtain such information and thereby keep the pace with the evolution of services and technologies.[57]

This view is, in a word, wrong. At most, the FBI's surveillance capabilities in the digital environment are limited to the capabilities possible in the analog environment. As we discuss in more detail below, the process by which the "standard" was adopted was largely closed to groups dedicated to protecting privacy rights; it is not surprising, then, that the resulting proposal for a standard would insufficiently guard these rights. The scope of these efforts make it clear that both the FBI "punch list" and the proposed industry "standard" are

---

what is more important – without attending illegality." *Berger*, 388 U.S. at 63.

56 *Id.*

57 FBI Petition, para. 45.

entirely deficient and should simply be rejected.[58] Simply put, the enhanced surveillance features sought through the "punch list" features are the result of an expansive view of the statute by the FBI; such a reading is contrary to the text, structure and history of CALEA as well as the historic limitations imposed by Title III and the Fourth Amendment.

1. Location Tracking Information

The most obvious example of the FBI's efforts to expand law enforcement surveillance capabilities under the guise of CALEA is the requirement that wireless service providers have location tracking capabilities for law enforcement purposes. During the industry standard-setting procedure, carriers acquiesced to the FBI's request that cellular, PCS and other wireless service providers provide information to law enforcement on the location of wireless telephone users. Wireless service providers will have the capability to provide this location information as a result of implementing the location tracking requirements for enhanced 911 services.[59] That industry will have the capability to identify a mobile telephone user's location does not mean, of course, that law enforcement is

---

58 This section addresses only those items in the industry standard and the FBI's punch list that pose the greatest risks to privacy. The decision not to address all requirements included in the industry standard and the FBI's punch list should not be read as condoning those requirements not discussed.

59 Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling, Report & Order and Further Notice of Proposed Rulemaking, 11 FCC Rcd. 18676 (1996), *modified in part on reconsideration,* Memorandum Opinion and Order, 12 FCC Rcd. 22665 (1997). It is not surprising that the telecommunications industry would consider agreement with law enforcement on a technology that it was providing for other purposes – industry thus could "give" an item to law enforcement without incurring a separate cost (and, indeed, could obtain funding for technology required for Enhanced 911 service as well). But the critical analysis is not whether the parties have agreed to this item but whether, as a matter of statutory construction, location information is meant to fall within the parameters of CALEA. It is clear that it does not.

therefore entitled to this information.[60] The Commission has an independent statutory obligation to not "rubber stamp" industry-law enforcement agreements. Rather, it must evaluate whether the elements of such an agreement are authorized by CALEA. The Commission must perform this statutory duty by independently assessing the law and the facts and not by accepting uncritically the views of any party submitting comments (regardless of the identity of the party).

As the FBI has acknowledged, CALEA was not intended to provide law enforcement with access to *new* surveillance capabilities that now exist as a result of technological developments. Rather, it was intended solely to allow law enforcement continued access to traditional surveillance capabilities despite technological changes. There is no question that location-tracking information is a *new* surveillance capability. It was not available to law enforcement at the time CALEA was enacted. And indeed, the legislative history of CALEA makes clear that location-tracking capability is not a requirement of the statute. The report by the House Judiciary Commission expressly states that CALEA "requires telecommunications carriers to ensure that their systems have the capability to . . . (2) Isolate expeditiously information identifying the originating and destination number of targeted communications, *but not the physical location of targets*[.]"[61] Further, during hearings that preceded the enactment of CALEA, the FBI acknowledged that CALEA did not mandate

---

60 This also highlights the importance of the role given to the Commission to protect privacy interests. Industry likely acceded to the FBI's request for location tracking information because wireless carriers were already implementing this capability for enhanced 911 purposes. In other words, the industry would not have to incur additional costs to provide location information to law enforcement. The industry was not focused on limiting the reach of CALEA or protecting privacy concerns.

61 H.R. Rep. No. 103-827 at 16 (emphasis added).

that carriers provide location-tracking information. FBI Director Freeh testified that call setup information:

> does not include any information that 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.[62]

All parties agree that CALEA was intended merely to maintain the status quo and not to expand law enforcement surveillance capabilities. As such, the requirements of CALEA cannot include that wireless services carriers provide location-tracking information to law enforcement.

It also bears noting that there may be non-telecommunications methods by which law enforcement can obtain location-tracking information from a particular suspect in a particular surveillance. Most obviously, of course, it can track the suspect simply by following her. It also can use a tracking technology that does not involve telecommunications, such as a global positioning satellite system. We are not expert in law enforcement and assume that those who are experts in surveillance can list a dozen other techniques for locating a suspect. This does not mean that the values to be protected by CALEA are any less vital, but that legitimate protection of these interests will not threaten law enforcement.

---

62 Digital Telephone and Law Enforcement Access To Advanced Telecommunications Technologies and Services: Joint Hearings on H.R. 4922 and S. 2375 Before the Subcommittee on Technology and the Law of the Senate Committee on the Judiciary and the Subcommittee on Civil and Constitutional Rights of the House Committee on the Judiciary, 103d Cong. 29 (1994).

2. Conference Calls

The FBI also seeks to expand the surveillance capabilities of law enforcement with regard to conference calls. Specifically, the FBI has requested that the Commission require carriers to provide law enforcement with the capability to monitor a conference call set up by the target subscriber even after that subscriber has ended his participation.[63] For example, where law enforcement is authorized to monitor's A's communications facilities, and A initiates a conference call with B and C and A later hangs up, the FBI wants the capability to continue monitoring any continuing communications between B and C. The FBI acknowledges that this would be an expansion of law enforcement's current capabilities, but nonetheless maintains that it falls under the obligations of CALEA.[64]

Section 103(a)(1) of CALEA requires carriers to provide law enforcement with "all wire and electronic communications carried by the carrier . . . to or from equipment, facilities or services of a subscriber . . . ."[65] The FBI contends, without providing any support, that a conference call continues to be carried by the subscriber's facilities and supported by the subscriber's service even when the subscriber has hung up.[66] The FBI notes that the target subscriber need not be on the line in order for law enforcement to intercept a communication occurring over the subscriber's facilities. This is true, but the communication must be occurring over the subscriber's facilities. Once the subscriber has

---

63 *See* FBI Petition at 27.

64 FBI Petition at 30.

65 47 U.S.C. § 1002(a)(1).

66 FBI Petition at 32.