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

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

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.
Shari Steele, Esq.
ELECTRONIC FRONTIER FOUNDATION
1550 Bryant Street
Suite 725
San Francisco, California 94103

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

Kurt A. Wimmer
Alane C. Weixel
Mark E. Porada

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 Jeannie Anna Court
Oak Hill, Virginia 20171

December 14, 1998

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 Department of Justice and 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.

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 communications 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 ("Title III") 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. The Commission should find that the industry's interim standard and the DoJ/FBI Petition frustrate the privacy interests of federal statutes and of the Fourth Amendment. We urge the Commission to reject the industry standard and the DoJ/FBI punchlist proposal and to exercise its duty under CALEA to protect the individual privacy that is a vital component of our nation's foundation.

This rulemaking proceeding represents the first opportunity for privacy interests to participate in the implementation of CALEA. Privacy interests did not have an effective voice in the proceedings that led up to the interim standard and the DoJ/FBI punchlist. In this *Further Notice of Proposed Rulemaking*, however, the Commission makes the apparently final decision that it does not intend to reexamine any of the "uncontested" technical requirements of the interim standard. The Commission's determination that it will not issue a traditional notice of proposed rulemaking explaining the standard it proposes to approve and seeking public comment on that standard ensures that the public – and in particular privacy interests – will have no opportunity to be effectively apprised of the contents of the standard that will determine the wiretap functions that will be built into the Nation's telecommunications system. Making this final decision in a notice of proposed rulemaking is inconsistent with the Administrative Procedure Act. Also, by foreclosing discussion of a standard arrived at solely by industry and law enforcement, the Commission undermines its responsibility to protect the public's privacy interests in implementing CALEA.

CONTENTS

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

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

To: The Commission

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

The Electronic Privacy Information Center ("EPIC"), the Electronic Frontier Foundation ("EFF") and the American Civil Liberties Union ("ACLU") urge the Commission to protect the privacy rights of American citizens as it exercises its congressionally mandated authority to assess whether the capabilities sought in the petition filed by the Federal Bureau of Investigation and the Department of Justice (the "DoJ/FBI Petition") satisfy the requirements of the Communications Assistance for Law Enforcement Act ("CALEA") to ensure the privacy and security of electronic communications. As we discuss in these Comments, the Commission has fundamental responsibility, mandated by law, (1) to protect the privacy interests of those using the Nation's telecommunications system, and (2) to adopt rules that encourage the provision of new technologies and services to the public. *See* CALEA, Sec. 107(b)(2)(4), 47 U.S.C. § 1006(b)(2). The Commission should promote these goals and protect Americans' privacy interests by finding that the interim standard adopted by industry and the DoJ/FBI's "punchlist" exceed the scope of CALEA and thus should be rejected.

EPIC, EFF and the ACLU are committed to protecting the privacy rights of Americans—rights that are at the core of this country's Constitutional heritage[1] 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. Indeed, in an era when the black rotary phone ruled the land, the Supreme Court held: "Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices."[2] Advanced telecommunications equipment and services dramatically multiply the number of private encounters that take place electronically and create the potential for government surveillance of these encounters to be more pervasive and invasive.

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.[3] Beginning with Section 705 of the Communications Act of 1934, Congress has set out clear rules protecting the privacy of communication and limiting the government's ability to intercept electronic communications surreptitiously.[4] In 1968, Congress established a framework to allow wiretapping of telephone

---

1 "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).

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

3 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.").

4 *See* 47 U.S.C. § 605 ("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").

traffic 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" or the "1968 Wiretap Act") that wiretapping was to be an investigative means of "last resort."[5] The Electronic Communications Privacy Act of 1986 ("ECPA") extended privacy protections to a new set of technologies such as email, cellular phones and paging devices – reflecting Congress's clear intent that privacy rights keep pace with technological advances.[6]

Congress enacted CALEA largely in response to the FBI's concern that new technologies could be used to thwart criminal investigations and that its surveillance capabilities should not be diminished as new technologies get deployed. As FBI Director Freeh testified, "the legislation was intended to preserve the status quo . . . to provide law enforcement no more and no less access to information than it had in the past."[7] 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,

---

[5] *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).

[6] 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").

[7] H.R. Rep. No. 103-827, pt. 1, at 22.

indeed, the responsibility to ensure that privacy interests are accorded the highest priority in the implementation of CALEA.[8]

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 DoJ/FBI Petition, these concerns were realized. Now, with the release of the Commission's Further Notice of Proposed Rulemaking,[9] the privacy of our Nation's communications is seriously at risk. The Commission has tentatively decided to adopt all of DoJ/FBI's "punchlist" items and to adopt the industry's interim standard – J-STD-025 – with the possible exception of the interim standard's treatment of packet-mode communications. In explaining its tentative conclusions, the Commission offers virtually no discussion of privacy interests. The Commission fails to explain how its tentative conclusions are consistent with the privacy protections embodied in CALEA, the Fourth Amendment and Title III of the 1968 Wiretap Act.

Privacy interests had no voice in drafting or adoption of the interim standard. Having been excluded from these earlier proceedings, it is imperative that privacy interests, as directed by Congress, be given full consideration by the Commission. Accordingly, the Commission must confront the privacy issues raised by the interim standard and the "punchlist" items. Although the Commission has indicated that it will not attempt to interpret statutes other than CALEA,[10] the Commission must harmonize CALEA with the constitutional and statutory limitations on the government's ability to design systems to facilitate electronic surveillance.

---

8 CALEA § 107(b)(2), 47 U.S.C. § 1006(b)(2).

9 Communications Assistance for Law Enforcement Act, CC Docket No. 97-231, *Further Notice of Proposed Rulemaking*, FCC 98-282 (November 5, 1998) (the "*Further Notice*").

10 *Further Notice*, ¶ 33.

The Commission may not implement requirements under the guise of CALEA that violate CALEA, the Constitution or Title III. Applying this standard, the Commission should find that the industry's interim standard and the DoJ/FBI Petition, if granted, would frustrate the privacy interests of federal statutes and of the Fourth Amendment. The DoJ/FBI Petition seeks surveillance capabilities that far exceed the capabilities law enforcement 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 punchlist items. We address below those items in the interim standard and the FBI's punchlist that raise the most serious threats to privacy.

I. ISSUES RAISED BY THE PROPOSED INTERIM STANDARD

A. The Commission is Obligated to Uphold CALEA'S Strict Privacy Protections for Packet-Mode Communications.

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 and informed by the policy choices reflected in the Communications Act of 1934, the Commission must implement CALEA in a manner that protects the American public's communications privacy to the greatest extent possible while, at the same time, provides for legitimate law enforcement needs. CALEA also reflects the unambiguous commitment of Congress that compliance with law enforcement's needs should not interfere with the tremendous benefits provided by telecommunications technology and services. This clear vote of Congress in favor of advanced technology is found throughout the Act. For instance, Section 103(b) establishes firm limits on how far law enforcement may go to ensure compliance with CALEA's capability requirements.[11] Similarly, Section 109(b) directs the Commission to consider, in determining

[11] Section 103(b)(1)(A) states that CALEA shall not require law enforcement "to require any specific design of equipment, facilities, services, features, or system configurations to be adopted by any (continued…)

"reasonably achievable," that "[t]he policy of the United States [is] to encourage the provision of new technologies and services to the public." In assessing the interim standard's treatment of packet-mode communications, the Commission is obligated to follow the balance that Congress sought to strike between these goals.

1. Permitting Law Enforcement To Obtain Call Content Information Without Proper Authorization Violates the Privacy Mandate of CALEA.

J-STD-025 provides that law enforcement must have access to call-identifying information for packet-mode communications, but it does not require telecommunications carriers to exclude call content information from packets before providing the packets to law enforcement over call data channels. In other words, under J-STD-025, a law enforcement officer with only a pen register order would be able to receive all of the contents of a subscriber's telephone conversations in addition to call identifying information. To obtain call content information under a wiretap order, however, law enforcement is required to satisfy a much more demanding standard than is required to obtain call-identifying information under a pen register/trap and trace device. The reason for this is obvious: electronic surveillance of conversations poses far greater threats to privacy than does surveillance of the telephone numbers called from a particular phone or the telephone numbers of calls placed to a particular phone. Law enforcement may obtain a pen register/trap and trace device order by demonstrating that the information "likely to be obtained is relevant to an ongoing criminal investigation being

---

provider of a wire or electronic communication service, any manufacturer or telecommunications equipment, or any provider of telecommunications support services." Similarly, subparagraph (B) states in simple terms that law enforcement, under the guise of CALEA, must not interfere with the ability of the American people to enjoy a rich variety of telecommunications equipment and services: "[Law enforcement shall not] prohibit the adoption of any equipment, facility, service, or feature by any provider (continued…)

conducted by that agency."[12] Law enforcement may obtain a wiretap order to seize call-content information only in connection with certain enumerated crimes and upon demonstrating that *probable cause* exists that a crime is being committed or about to be committed by a particular individual and that communications concerning that offense will be obtained through the wiretap.[13] Law enforcement must also demonstrate that other investigative techniques have failed or are too dangerous.[14] The Commission correctly noted that allowing law enforcement with a pen register/trap and trace device order to obtain the call content of packet-mode communications violates the mandate in Section 103(a)(4)(B) of CALEA that telecommunications carriers provide information to law enforcement "in a manner that protects . . . the privacy and security of communications . . . not authorized to be intercepted."[15]

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. Though nearly all of the issues before the Commission involve some aspect of new technology, the undersigned parties representing privacy interests believe that these profound concerns and competing objectives apply with special force to the current cutting-edge technology of packet-mode service. In order to balance these objectives, Congress followed the structure of Title III of the 1968 Wiretap Act and accordingly limited the ability of law enforcement to intercept communications.

---

of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services."

12 18 U.S.C. § 3122(b).

13 18 U.S.C. § 2521(c)(3).

14 *Id.*

15 *Further Notice*, ¶ 63.

CALEA imposes four requirements on the telecommunications industry. Three of the requirements are intended to "preserve" -- not expand or enhance, but "preserve" -- law enforcement's surveillance capabilities and the fourth, equally important, is intended to uphold the privacy interests of the American public. [16] 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) (emphasis added).

Moreover, 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.[17] 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. Indeed, notwithstanding CALEA, it

---

[16] 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 communications services and technologies.").

[17] H. R. Rep. No. 103-827 at 22.

remains a violation of the Communications Act, punishable by fine of up to $100,000, to unlawfully divulge information about the existence or content of communications by wire or radio. In light of this long-standing decision in favor of privacy, Congress directed the telecommunications industry, law enforcement and the Commission "to narrowly interpret" the requirements of CALEA.[18]

To require telecommunications carriers to provide call identifying information without also requiring that call content information be withheld when law enforcement is authorized to receive only the former would undermine entirely the privacy protections included in CALEA. As the Commission stated, "packet-mode telecommunications are expected to grow rapidly in the near future."[19] The escalating need for high-speed data transmission services will likely spur the development of packet-mode systems. If the distinction between call-identifying information and call-content information is completely eroded for packet-mode communications, the privacy protections implemented by Congress and courts and relied on by subscribers may all but disappear. This outcome would be most unfortunate from the perspective of the American public, which have come to rely increasingly on advanced packet-mode services for their critical telecommunication needs.[20]

---

[18] *Id.* at 23.

[19] *Further Notice*, ¶ 63.

[20] During 1996, 3,262 federal pen register orders were approved, which affected the telephone facilities of 7,070 people. The same year, 1,307 federal trap and trace orders were approved, which affected the telephone facilities of 3,450 people. Letter from Department of Justice to Hon. Orrin Hatch, April 14, 1997. Under the interim standard, the call content of conversations affecting more than 10,000 individuals – if carried over packet-mode systems – would have been released to law enforcement without proper authorization. By way of contrast, only 581 federal wiretaps were executed in 1996, affecting the facilities of 1,149 people.

When CALEA was enacted in 1994, packet-mode systems were not widely used for telecommunications purposes. This was not one of the technological advances identified by the FBI as hindering surveillance capabilities, and accordingly CALEA was not enacted to address specifically access to telecommunications carried on packet-mode systems. In sum, there is nothing in the statute or the legislative history that justifies granting packet-mode communications an exception from CALEA's requirement that telecommunications carriers protect the privacy of communications not authorized to be intercepted. At minimum, neither the Commission nor law enforcement, nor, for that matter, the industry, has sufficient experience operating packet-mode systems to establish intelligent standards for wiretaps in this area. If DoJ/FBI desire an exception for packet-mode telecommunications from the requirement in CALEA that carriers provide privacy and security for communications not authorized to be received, they must obtain such an exception from Congress.

The Commission should reject the DoJ/FBI bid for call-identifying plus content information because providing the call-identifying information is not "reasonably achievable." Pursuant to CALEA, a carrier must isolate and provide law enforcement authorization to call-identifying information "that is reasonably available to the carrier."[21] If call-identifying information cannot be separated from call-content information, then it is not "reasonably available" and therefore should not be provided. DoJ/FBI have failed to satisfy their burden of establishing that call-identifying information is readily available. Until DoJ/FBI meet this burden, call-identifying information for packet-mode systems should be excluded from the capability requirements of CALEA.

---

[21] CALEA § 103(a)(2), 47 U.S.C. § 1002(a)(2).

2. Permitting Law Enforcement to Obtain Call Content Information in Packet-Mode Communications Without Proper Authorization Violates the Fourth Amendment and Title III of the 1968 Wiretap Act.

Allowing law enforcement to obtain call content information with only a pen register represents a dangerous expansion of law enforcement and would violate the "particularity" requirements of the Fourth Amendment and Title III of the 1968 Wiretap Act. Subjects of electronic surveillance are protected by the Fourth Amendment's restrictions on searches and seizures. In *Berger v. New York*, the Supreme Court held that lengthy, continuous or indiscriminate electronic surveillance violated the Fourth Amendment.[22] 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.[23]

Title III of the 1968 Wiretap Act, which was enacted a year after *Berger* and *Katz*, was Congress' response in the form of national legislation to a body of law "totally unsatisfactory in its consequences" for privacy and justice.[24] 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.[25] 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 not even

---

22 388 U.S. 41 (1967).

23 389 U.S. 347 (1967).

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

25 *Id.* at 66.

be relevant to an investigation much less contemplated by a court order. Electronic surveillance also tends to extend for long stretches of time. Moreover, it is conducted surreptitiously and without notice to 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."[26] To mitigate some of the more dangerous characteristics of electronic surveillance, among other things, Title III requires that government surveillance must be, *inter alia*, for limited periods of time, for specified crimes, and only as a last resort.[27]

Title III's privacy safeguards in the form of particularity 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."[28] The *Berger* Court found that New York's eavesdropping statute was a "blanket grant of permission . . . without adequate judicial supervision or protective procedures."[29] 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.[30] "Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices."[31]

---

[26] *See Richards v. Wisconsin,* 117 S. Ct. 1416 (1997).

[27] *See* 18 U.S.C. § 2518(3). In addition, Title III requires that government surveillance minimize the interception of innocent communications. 18 U.C.S. § 2518(5).

[28] *Berger v. New York*, 388 U.S. 41, 56 (1967).

[29] *Id.* at 59.

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

[31] *Berger,* 388 U.S. at 63.

Allowing law enforcement to obtain the full content of customer communications from carriers using packet switching even when the government is authorized to intercept only addressing or signaling data would permit the same type of indiscriminate electronic surveillance found unconstitutional in *Berger*. Law enforcement would be given a "blanket grant of permission" to review call content without being subject to adequate judicial supervision or the protective procedures of Title III.

The answer that law enforcement would minimize unauthorized communications obtained by surveillance methods is inadequate. Were the framers of our Constitution confident that law enforcement would not engage in unwarranted searches and seizures, they would not have included the Fourth Amendment. Were Congress confident that law enforcement personnel would scrupulously avoid all unauthorized communications, it would not have adopted the privacy mandates in CALEA or Title III.[32] Instead of relying on blind faith, Congress adopted safeguards to protect the privacy of Americans. Those safeguards are enshrined in Title III and CALEA, and should not be abandoned in this proceeding.

B. The Location Tracking Provisions Contained in the Industry Standard Are Neither Contemplated Nor Permitted Under CALEA, and Law Enforcement Access to that Information Without a Warrant Would Result in an Unconstitutional Invasion of Privacy.

The industry standard contains provisions that would identify the location of a cellular telephone user's "mobile terminal." As the Commission noted in the *Further Notice*, the industry

---

[32] Experience shows that law enforcement personnel sometimes misuse information obtained by electronic surveillance. By way of example, the Los Angeles police department and the Los Angeles District Attorney's Office are currently under a firestorm of criticism for engaging in a hidden practice known as "hand-off." A "hand-off" occurs when the police, while conducting electronic surveillance on Person A obtain incriminating information on Person B and pass that information on to other police officers as a "tip." Under this practice, Person B was never advised that his conversations had been picked up by electronic surveillance. This practice raises serous constitutional concerns, and illustrates (continued…)

standard provision is vaguely written.[33] The standard does not state whether telecommunications carriers would be required to track the precise location of the handset or the location of the cell site to which the handset is connected. The Commission's statement that law enforcement and the industry "appear now to agree that the standard covers only the location of the cell site, and only at the beginning and termination of a call,"[34] and its suggestion that location tracking information would be available to law enforcement "irrespective of whether a call content or call data channel was employed,"[35] highlight the confusion concerning the scope of the location tracking provision contained in the industry standard.

It is clear from CALEA's language and its legislative history that Congress did not intend for law enforcement to gain access to location tracking information under the statute. The statute plainly states that, to the extent telecommunications carriers are obliged to facilitate law enforcement access to "call identifying information," such 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*)."[36] The House Judiciary Committee Report plainly states that CALEA "requires telecommunications carriers to ensure that their systems have the capability to . . . [i]solate expeditiously information identifying the originating and destination number of targeted communications, *but not the physical location of targets*[.]"[37]

---

the need for judicial scrutiny of surveillance practices. *See* M. Cooper, "Wired," NEW TIMES OF LOS ANGELES (Aug. 13, 1998).

33 *Further Notice,* ¶ 54.

34 *Id.*

35 *Id.* ¶ 48.

36 CALEA § 103(a)(2)(B), 47 U.S.C. § 1002(a)(2)(B) (emphasis added).

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

It is obvious that Congress did not contemplate in CALEA the release of location tracking data to law enforcement. Rather, Congress recognized that if law enforcement requires tracking information to assist in a criminal investigation, it must obtain a warrant that satisfies Fourth Amendment and Title III standards.[38]

The DoJ/FBI position in this proceeding is particularly surprising, given its contradictory statements made during hearings as Congress was debating CALEA. FBI Director Freeh testified that call setup or identification 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.[39]

The FBI cannot assert, when testifying before Congress, that CALEA does not require or even permit telecommunications carriers to provide location tracking information to law enforcement, and then claim the exact opposite after Congress acted in reliance upon the FBI's assurances. To accept law enforcement's arguments at this stage would permit the FBI to complete an end-run around the legislative process and Congress's reliance on the testimony of FBI Director Freeh.

---

[38] A determination that CALEA was not meant to require production of location tracking information does not make the specific provision in § 103(a)(2)(B) dealing with tracking information in the context of pen registers "mere surplusage," as the Commission suggests. *See Further Notice* at 28 n.106. It is clear from the legislative history that Congress, and the FBI, did not intend for CALEA to require telecommunications carriers to make available location tracking data; law enforcement is limited to the means of access available under Title III and the Fourth Amendment. Section 103(a)(2)(B) simply clarifies that, to the extent law enforcement obtains a pen register pursuant to statutes other than CALEA, such pen register will not entitle the government to access any location tracking information.

[39] 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).

Regulations requiring location tracking information not only would violate the terms of the statute and congressional intent, but also would interfere with privacy interests shielded by the Fourth Amendment. The Supreme Court has held that governmental agents violate the Fourth Amendment when they use tracking devices to locate people or property in private areas. In *United States v. Karo*,[40] law enforcement agents installed a tracking device into a container of chemicals sold to an unwitting buyer. The agents then used the tracking device to follow the buyer's movement into his private residence.

The Court drew a sharp distinction between the use of a tracking device to follow an individual's movement in public areas and in areas "not open to visual surveillance."[41] The Court stated that "[i]ndiscriminate monitoring" of a person's or his property's location in areas "withdrawn from public view would present far too serious a threat to privacy interests" protected under the Fourth Amendment.[42] Visual surveillance might enable government agents to confirm that a person has entered into a private residence or other protected area, but location tracking equipment reveals a "critical fact about the interior of the premises that the Government is extremely interested in knowing and that it could not have otherwise obtained without a warrant."[43]

It is obvious that law enforcement would benefit from acquiring location tracking information from telecommunications carriers without the burden of securing a warrant, but its

---

40 468 U.S. 705 (1984).

41 *Id.* at 714; *see also United States v. Knotts*, 460 U.S. 276, 284 (1983) (permitting the use of a tracking device where the suspect was travelling only on public roads and where there was "no indication that the [device] was used in any way to reveal information as to the movement … within the cabin, or in any way that would not have been visible to the naked eye from outside the cabin").

42 *Karo*, 468 U.S. at 716.

43 *Id.* at 713.

argument "is based upon its depreciation of the benefits and exaggeration of the difficulties associated with procurement of a warrant."[44] Investigative efficiency, while important for law enforcement purposes, is not sufficient justification for overriding fundamental privacy interests protected by the Fourth Amendment.[45] CALEA does not contemplate the provision of any location tracking information, let alone the indiscriminate form of tracking sought by the DoJ/FBI.

Law enforcement has been surviving without telephone location tracking information for centuries. DoJ/FBI readily concede that CALEA "does not expand law enforcement agencies' power or authority to conduct electronic surveillance; that authority continues to be defined principally by Title III."[46] It is clear that law enforcement has never utilized location tracking information before and the use of such technology would, in fact, *expand* the government's ability to conduct electronic surveillance while making traditional methods of surveillance unnecessary. As such, Congress did not consider and CALEA does not permit regulations enabling law enforcement to gain access to that information.

DoJ/FBI argue that it has been able to obtain the "location" of callers in the wired environment whenever it has pen register or trap and trace authority, because the telephone number that is revealed is associated with the particular address at which a caller must be located. But it is not convincing to state in a conclusory fashion that location information is available in a wired environment and therefore the same information should be available in a

---

44 *Id.* at 717

45 *See id.* at 718 (noting that the "argument that a warrant requirement would oblige the Government to obtain warrants in a large number of cases is hardly a compelling argument against the requirement").

46 DoJ/FBI Joint Petition for Expedited Rulemaking, at 19.

wireless environment.[47] The fundamental purpose of pen register or trap and trace orders is to provide law enforcement with the identity of callers, not their physical location. The location information that is revealed in a wired setting is simply a by-product of that environment, where each telephone number is assigned to a physical location. Access to a wired telephone number automatically provides access to the physical location of the telephone.

In a wireless environment, standard pen register or trap and trace authority can still reveal the information lawfully sought by DoJ/FBI: the telephone number of originating and terminating traffic. At the same time, there is no physical location automatically associated with a cellular telephone number, so law enforcement cannot obtain that information by default. Because of the mobility involved in wireless communications, however, the physical location of a caller may reveal sensitive or confidential information concerning the caller's travels that law enforcement has no right to receive under the limited authority of a pen register or trap and trace order. For instance, a cellular caller may be using his telephone in his attorney's office while conducting privileged business or from the home of a romantic partner. Law enforcement should not be allowed to follow an individual's daily movements through private areas simply because the individual happens to use his cellular telephone. If law enforcement officers wish to track someone, they can use traditional surveillance methods and stakeouts to follow a person's progress through public areas.

---

[47] The widespread use of cordless telephones, including those that enable a person to go several hundred feet (and some claim one mile) from the telephone's base station, demonstrate that location information is a mere artifact of the wired world and not an immutable fact of telecommunications networks. For example, cordless phones operating at 900 MHz and newer phones operating at 2.4 GHz can permit a participant on a "wired" telephone to be quite distant from their wired bases (and even in the homes of others, particularly in apartment buildings).

DoJ/FBI have suggested that telecommunications carriers already will have the capability of tracking an individual's location through implementation of the tracking requirements for enhanced 911 ("E911") services.[48] Under the telecommunications industry's E911 obligations, it will be possible to determine a mobile telephone user's location when the user dials 911. That the industry will have the capability of determining a user's location when the user has initiated a call to emergency personnel, however, does not mean that the technology should, or even could, be used to track that user's location when there has been no call to 911. The industry's E911 obligations can be satisfied in ways that do not accomplish the routine tracking results sought by law enforcement, so it is incorrect to assume that the industry already will have the capability to track locations whenever a cellular telephone is turned on or in use.

E911 tracking will not operate as a general homing device, monitoring a cellular user's location at all times when the telephone is in use. Rather, the E911 tracking capability will only be activated when an emergency call is initiated by the user. By dialing 911, the cellular telephone user implicitly has consented to having his location tracked. But the DoJ/FBI Petition turns this life-saving service on its head. DoJ/FBI envision a far different form of tracking, one which could be activated without the user's knowledge and which could track the user in non-emergency situations. In that context, the cellular user certainly has not consented to being tracked and there has been no waiver of the user's right to travel in private areas free from governmental monitoring.

The fact that the telecommunications industry may have consented to the DoJ/FBI request to develop technology that can track telephone users' locations twenty-four hours a day

---

[48] 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).

does not in any way alter the conclusion that wireless telephone users' privacy rights are jeopardized by the industry standard. The Commission is obligated to examine each issue closely, and it should not easily be swayed by industry acquiescence. The industry may have financial or business-related reasons to go along with the DoJ/FBI request, but those reasons do not take into account the privacy interests of cellular users. The industry's willingness to develop technology that it is already partially required to develop in order to fulfill its E911 duties does not foreclose the Commission's statutory duty to examine the industry standard and protect the "privacy and security of communications and call-identifying information not authorized to be intercepted."[49] The Commission must exercise its duty and reject the industry standard for location tracking information.

II. ISSUES RAISED BY THE DoJ/FBI "PUNCHLIST"

A. Expanded Access to Conversations of Participants in Subject-Initiated Conference Calls Is Inconsistent with Statutory and Constitutional Limitations.

The Commission's tentative conclusion to require that law enforcement have the ability to monitor conversations connected via conference call even after the subject, or someone using the subject's facilities, drops off significantly expands Title III's "facilities" doctrine. Title III permits law enforcement to monitor conversations taking place over the facilities of the intercept subject. "Facilities" have traditionally been considered for Title III purposes as the subscriber's terminal equipment.[50] The DoJ/FBI Petition seeks to expand the "facilities" doctrine to include a

---

[49] CALEA §§ 103(a)(4)(A) & 107(b)(2), 47 U.S.C. §§ 1002(a)(4)(B) & 1006 (b)(2).

[50] *See, e.g.*, *United States v. Petti*, 973 F.2d 1441 (9th Cir. 1992) (noting that for a "roving" wiretap under 18 U.S.C. § 2518(11)(b)(ii), "[o]nly telephone facilities actually used by an identified speaker may be subjected to surveillance[.]"); *United States v. Abramson, 553 F.2d* 1161, 1164 (8th Cir. 1977) (noting that the target facilities were two telephones), *cert. denied,* 433 U.S. 911; *see also United States v. Tavarez,* 40 F.3d 1136, 1139 (10th Cir. 1994) (interpreting "facilities" as used in an Oklahoma wiretap statute to mean the target telephones).

subscriber's facilities and *services and any network facilities that support the subscriber's services.*

For example, when a subscriber initiates a conference call, a "conference bridge" is allocated to the conversation from a "pool" of similar bridges located at the local exchange carrier's switch. These bridges are shared by all subscribers of the conference calling service. According to current practice of law enforcement and consistent with the FCC's precedent, the "subscriber facility" is the connection between a subscriber's phone and the subscriber side port of the carrier's switch. Beyond that point, only network resources are used. Thus, the law enforcement agency with authority to monitor only the *subject's* facilities is not permitted to trace conversations on those network resources once the subscriber disconnects. The fact that law enforcement currently hears three parties on a conversation of a tapped line is a function of all the conversations appearing on the target's side of the bridge, not that the law enforcement authority is actually in the middle of the bridge. If the target disconnects, his or her facility also is disconnected; thus, the law enforcement authority has no connection to the subscriber's facility that built the conference call bridge.

However, under the DoJ/FBI's interpretation of CALEA's requirements, any conference call initiated by the target's facilities would be subject to an ongoing intercept even after the target – or someone using the target's phone – disconnects. Thus, carriers would have to provide access to any continuing conversations between the other participants of the conference call. Pursuant to CALEA, law enforcement, with appropriate authorization, is entitled 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."[51]

(continued…)

Interpreting the word "services" to expand dramatically the facilities doctrine cannot be squared with Congress' intent in adopting CALEA or the limitations of the Fourth Amendment.

1. Expanded Access to Conference Call Content Is Inconsistent with CALEA.

In adopting CALEA, Congress intended the assistance requirements to be "both a floor and a ceiling."[52] Congress took special notice of the statement by the FBI Director 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 that it had in the past."[53] Congress "urge[d] against overbroad interpretation of [CALEA's] requirements," and stated that it "expects industry, law enforcement and the FCC to narrowly interpret the requirements."[54]

The DoJ/FBI Petition seeks to expand law enforcement surveillance capabilities to include conversations between participants in a conference call that are no longer using the equipment or facilities of the intercept subject. The DoJ/FBI Petition has requested that the Commission require carriers to provide law enforcement with the capability to monitor a conference call, which was set up using the subject's facilities, after the person using the subject's facilities has hung up or placed the other participants on hold. In other words, the DoJ/FBI Petition seeks to monitor conversations that cannot be heard over the intercept subject's facilities. Though DoJ/FBI acknowledge that this would be an expansion of law enforcement's current capabilities, they nonetheless maintain that it falls under the obligations of CALEA.[55]

---

51 CALEA § 103(a)(1), 47 U.S.C. § 1002(a)(1).

52 H.R. Rep. No. 103-827, pt. 1, at 22 (1994).

53 *Id.*

54 *Id.* at 22-23.

55 DoJ/FBI Petition at 32.

The Commission's tentative conclusion adopting the DoJ/FBI Petition's interpretation fails to justify this expansion of the "facilities" doctrine in light of the direct instruction from Congress that the Commission should "narrowly interpret" the requirements of CALEA. Indeed, the Commission appears uncomfortable accepting DoJ/FBI's interpretation of the term "services" to include network facilities because that expanded interpretation could have far-reaching implications. In the *Further Notice*, the Commission has proposed limiting a carrier's requirement to provide to law enforcement the call content of the remaining parties to a conference call after the target – or someone using the target's telephone – drops off only when "the call nonetheless remains routed through the subscriber's 'equipment, facilities or services.'"[56] If the conversation between the remaining parties is either disconnected or rerouted so that the "equipment, facilities or services of the subscriber" are no longer used to maintain the conference call, carriers would not have to provide law enforcement with access to the remaining call content.[57]

In other words, the Commission appears to be reaching for a requirement that call content of a conference call be provided only when the target's "facilities" are being used. Because CALEA was not intended to expand surveillance capabilities, the definition of "facilities" should continue to be limited to a subscriber's terminal equipment. Once the target's terminal equipment is no longer in use, surveillance of the call ceases. Accordingly, once a target puts a conference call on hold (or disconnects), both the target's and law enforcement's ability to hear other parties should terminate.

---

56 *Further Notice*, ¶ 78.

57 *Id*.

2. Expanded Access to Conference Call Content Violates the Fourth Amendment.

Expanded access to conference call content would also violate the privacy protections of the Fourth Amendment. Allowing law enforcement to continue to listen to the conversation of participants to a conference call after the subject's facilities have been disconnected would amount to giving law enforcement "a roving commission to 'seize' any and all conversations" without having established probable cause to do so.[58] "The purpose of the probable-cause requirement of the Fourth Amendment is to keep the state out of constitutionally protected areas until it has reason to believe that a specific crime has been committed[.]"[59] If law enforcement may monitor conversations between individuals who are not subject to a surveillance order and who are not using facilities that are subject to a surveillance order, the probable-cause requirement would be wholly avoided. Surveillance would not be circumscribed, but instead would amount to a fishing expedition, with law enforcement listening to conversations that involve neither the intercept subject nor his or her facilities for any potential criminal activity. Such surveillance violates the particularity requirement and the probable cause requirement of the Fourth Amendment.

B. Signaling Information Falls Outside the Definition of Call-Identifying Information.

DoJ/FBI seek to sweep within the definition of "call-identifying information" other types of signaling information that fall outside the scope of CALEA. The legislative history clarifies that call-identifying information is limited to "electronic pulses, audio tones, or signaling messages that identify the numbers dialed or otherwise transmitted for the purpose of routing

---

58 *Berger v. New York*, 388 U.S. at 59.

59 *Id*.

calls through the telecommunications carrier's network."[60] The legislative history further clarifies that in pen register investigations, call-identifying information refers to the pulses, tones or messages that "identify the numbers dialed from the facility that is the subject of the court order."[61] In trap and trace investigations, call-signaling information refers to incoming pulses, tones or messages that "identify the originating number of the facility from which the call was placed and which are captured when directed to the facility that is the subject of the court order."[62] To emphasize that call-signaling information is limited to pulses and tones that identify incoming or outgoing phone numbers, Congress further stated that "[o]ther 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."[63]

Despite this clear statement of Congressional intent, DoJ/FBI seek to expand the definition of call-signaling information beyond the signals and tones initiating a call to include signal and tones used "to manipulate the call."[64] For example, DoJ/FBI request that carriers be required to notify law enforcement when the subject has pressed the flash hook indicating call waiting or the placing of a party on hold.[65] DoJ/FBI also want carriers to provide party hold, party join and party drop messages. As these signaling tones do not identify the telephone number dialed by the subject subscriber or the telephone numbers of incoming calls to the

---

60 H.R. Rep. No. 103-827 at 21.

61 *Id.*

62 *Id.*

63 *Id.*

64 DoJ/FBI Petition at 36.

65 DoJ/FBI Petition at 34.

subject subscriber, they exceed the scope of CALEA. "In pen register investigations, these pulses, tones or messages identify the numbers dialed from the facility that is the subject of the court order . . . . 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."[66]

The Commission's tentative conclusion that such signaling information "identifies the origin, direction, destination or termination" of a communication and therefore must be made available under CALEA is inconsistent with the legislative history of CALEA and expands the type of call-identification information traditionally available to law enforcement. As is true with a number of other bits of information discussed in this proceeding, law enforcement may be able to obtain this kind of information with the appropriate court order, but that conclusion does not mandate that such information necessarily be made under CALEA. Neither the Commission nor CALEA is the sole means to satisfy law enforcement's legitimate need for information. Because Congress directed the Commission to interpret CALEA narrowly, this expansion is unwarranted.

C. CALEA Does Not Permit Law Enforcement to Obtain Post-Cut-Through Digits Through a Pen Register Order Directed at the Initial Telecommunications Carrier.

DoJ/FBI seek regulations requiring telecommunications carriers to provide law enforcement with post-cut-through dialed digits,[67] arguing that the digits amount to "call identifying information" under CALEA. The dialed digits sought by law enforcement do not

---

[66] *See* H.R. Rep. No. 103-827 at 21.

[67] Post-cut-through dialing information contains the numbers an individual dials after a call circuit has been completed by the initial carrier. In particular, law enforcement is interested in acquiring the post-cut-through dialed digits when an individual dials an 800-number to reach a long distance provider, (continued…)

qualify as "call identifying information," nor are they "reasonably available" to carriers. For both reasons, the Commission must reject DoJ/FBI's request for regulations requiring disclosure of this information.

CALEA defines "call identifying information" as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier."[68] Comments from the telecommunications industry universally establish that, from the initial carrier's standpoint, the call is outside the purview of the initiating carrier once the subscriber has connected to the long distance carrier.[69] As the FCC has acknowledged, the initial numbers dialed to reach the long distance provider are transmitted over the initial carrier's call data channel, but the second set of numbers dialed once the subscriber is connected to the long distance provider are transmitted along with voice and other content on the initial carrier's call content channel.[70]

The post-cut-through numbers are carried on the initial carrier's call content channel, so they must be treated the same as other call content and not revealed to law enforcement through a pen register order served on the local carrier.[71] Because the post-cut-through digits are transmitted in the call content portion of the local provider's transmission, access to that

---

and then, after the cut-through to the long distance provider, dials the telephone number of the ultimate party he seeks to reach.

68 CALEA § 102(2), 47 U.S.C. § 1001(2).

69 *See, e.g.*, U S West Comments, at 15-17.

70 *Further Notice*, ¶ 128.

71 *See, e.g.*, TIA Comments, at 44 ("[F]or a local exchange carrier, it is irrelevant whether post-cut-through communications consist of dialed digits, a fax transmission, or a whispered conversation between two lovers.").

information must be analyzed as if law enforcement were trying to access any other call content. Information contained in the call content portion of a transmission does not qualify as "call identifying information," because it does not identify the "origin, direction, destination or termination" of the initial carrier's communication.[72] The digits dialed by the subscriber once he or she has connected to the long distance carrier may qualify as "call identifying information" for the long distance carrier, but not for the local telecommunications service.

In many cases, post-cut-through digits may reveal credit card numbers, personal identification numbers, bank account numbers and information, responses to automated systems, substantive messages sent to pagers or other content-laden data that has nothing to do with the ultimate telephone number being dialed. Clearly this information, along with the conversations themselves contained in the call content channel transmission, exceeds the scope of "call identifying information" under CALEA. The Justice Department has conceded in another context that "electronic impulses" transmitted after a telephone call has connected to the called party are "substantive in nature" and "are the 'contents' of the call."[73] The government appears to be in agreement, then, that digits entered after the caller has connected to the long distance carrier contain information that does more than identify the "origin, direction, destination, or termination" of a call, as required for "call identifying information."

Law enforcement apparently desires to sweep all of this substantive content under the heading of "call identifying information," which would permit government access to post-cut-through digits with only a pen register order. It is clear that a pen register order only permits law enforcement agencies to access "electronic or other impulses which identify the numbers dialed

---

[72] CALEA § 102(2), 47 U.S.C. § 1001(2).

or otherwise transmitted on the telephone line."[74] To the extent that post-cut-through digits are contained in call content channel transmissions, law enforcement has no authority to access them with nothing more than a pen register order. The Commission should reject the FBI's attempt to gain through the back door what it otherwise is prohibited from obtaining directly. Post-cut-through digits are not "call identifying information" under CALEA. The Commission must exercise its duty under CALEA to protect the "privacy and security of communications and call-identifying information not authorized to be intercepted."[75]

Even if it finds that post-cut-through digits qualify as "call identifying information," the Commission should reject DoJ/FBI's approach. Telecommunications carriers are only required to ensure that their equipment is capable of "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*."[76] The legislative history is clear that "if such information is not reasonably available, the carrier does not have to modify its system to make it available."[77] CALEA was "not intended to guarantee 'one-stop shopping' for law enforcement."[78]

Members of the telecommunications industry are in agreement that technology currently does not permit the initial carrier to separate post-cut-through digits used to dial the final party's telephone number from other digits or content contained in the call content channel

---

73 Letter from Ann M. Harkins, Acting Assistant Attorney General, U.S. Department of Justice, to Hon. Henry J. Hyde, Chairman, House Judiciary Committee 2-3 (May 20, 1998) (attached as Ex. A).

74 18 U.S.C. § 3127(c).

75 CALEA § 103(a)(4)(A), 47 U.S.C. § 1002(a)(4)(A).

76 CALEA § 103(a)(2), 47 U.S.C. § 1002(a)(2) (emphasis added).

77 H.R. Rep. No. 103-827, at 22.

78 *Id.*

transmission.[79] Currently, telephone switches use a "tone receiver" to detect dialed digits. Once a call is cut through to the recipient of the call (whether the recipient is another person or an automated long distance carrier), the tone receiver is disconnected from the call circuit and is available for use on other calls. As TIA pointed out, "it would require major system modifications to dedicate a tone receiver for the duration of each call, which would be necessary to detect post-cut-through digits and deliver them to law enforcement."[80] With the advent of new technology, such as voice-recognition dialing, the difficulty and expense in discovering and recording post-cut-through digits will only increase.[81]

Vendors have advised that the development costs for digital dial extraction technology that could separate digits used to dial a second telephone number from other material contained in the call content channel would likely exceed the development costs for all of the other items contained in DoJ/FBI's punchlist.[82] The Commission is only authorized to issue regulations that implement the requirements of CALEA "by cost effective methods."[83] Clearly, there is no cost-effective way to require telecommunications carriers to separate certain post-cut-through digits from other call content, so regulations requiring such an end are inappropriate.

The industry has shown that such technology currently does not exist and would be extremely expensive to develop. The burden lies with law enforcement, which concedes that post-cut-through digits are contained in call content channel transmissions that are excluded from

---

79 *See* TIA Comments, at 44-45; U S West Comments, at 15-16; AirTouch Comments, at 10-11.

80 TIA Comments, at 44.

81 *See* TIA Comments, at 45 ("Carriers have no way to implement such technical solutions, nor do they have any business reason to do so.").

82 *See* AirTouch Comments, at 18; U S West Comments, at 22 (discussing expensive costs involved in providing all information sought by law enforcement on call data channel).

83 CALEA § 107(b)(1), 47 U.S.C. § 1006(b)(1).

CALEA, to establish that reasonable means exist to limit the data received from the call content channel to the final telephone number dialed. If law enforcement cannot meet its burden, then it cannot obtain access to post-cut-through digits.

DoJ/FBI may argue that its ability to investigate potential crimes is being thwarted by clever suspects who intentionally route their calls through long distance carriers to evade pen registers attached to their local service. The Commission must reject law enforcement's contention that it should be free under CALEA to receive post-cut-through digits that are interwoven with call content without a warrant simply because "there is justification in the facts for believing that a crime is being or will be committed and that monitoring the [call] wherever it goes is likely to produce evidence of criminal activity."[84] CALEA does not permit such access simply to make law enforcement investigations easier or less burdensome.

DoJ/FBI also argue that law enforcement has had access to call content in the analog environment with only a pen register order, and law enforcement officers have selectively chosen not to listen to call content once they have identified the parties involved in the conversation. To the extent that that situation occurs, it is an abnormality of the analog environment and should not be extended to digital communications. While many law enforcement officers execute their duties in a manner faithful to their constitutional and legal obligations, the law does not permit government agents to police their own conduct entirely free from outside supervision. In a number of well-publicized situations, law enforcement officers have flagrantly and systematically disregarded their duty to minimize intrusions into the private electronic

---

[84] *Karo*, 468 U.S. at 717.

communications of individuals who were not even criminal suspects.[85] If technology currently does not allow telecommunications services to separate post-cut-through digits used to dial a second telephone from the remainder of the call content channel transmission, law enforcement has no authority under CALEA to obtain access to those digits.

DoJ/FBI argue that any information pertaining to the ultimate telephone number with which the suspect connects is "call identifying information," regardless of the channel in which the information is transmitted. An example shows the far-reaching implications of DoJ/FBI's proposal. Assume a target dials an 800-number to reach a long distance provider. Rather than typing in the telephone number he seeks to reach, he waits for the long distance operator to pick up, and asks the operator to complete the call. Under DoJ/FBI's reasoning, the conversation between the suspect and the operator would be "call identifying information," because it would involve the "direction" or "destination" of his initial call.

It should be obvious that actual conversations between two people amount to call content, not "call identifying information." If DoJ/FBI's position were adopted, however, the line between the two would be impermissibly and dangerously blurred. The Commission must not

---

[85] In a notorious case currently developing in Los Angeles, a judge ordered the district attorney's office to reveal to defense attorneys the Los Angeles Police Department's "handoff" tactic. A "handoff" occurs when police officers monitoring a wiretap of a suspect's telephone line uncover information about an unrelated individual. The officers "handoff" the information to a second set of officers, without identifying the source of the information—a wiretap. The second group of officers then initiate an investigation of the individual to uncover independent evidence of wrongdoing, without having direct knowledge that the initial information came from a wiretap. *See* Greg Krikorian, "Wiretap Ruling Rocks L.A. Legal, Police Circles," Los Angeles Times, B1 (Apr. 8, 1998). The "handoff" technique allows officers to circumvent requirements under federal and state law that require them to disclose the existence of a wiretap to those whose conversations are being monitored, because the investigating officers can claim they did not rely on any wiretap in developing their case against the suspects. The district attorney's office acknowledged that officers refused to inform suspects that their telephones had been tapped in "handoff" procedures in 58 cases since 1993. There are estimates officers conducted "handoffs" in many more situations that never led to any arrests. *See* "Case in Los Angeles Raises Concerns Over (continued…)

succumb to law enforcement's attractive argument that its proposals must be adopted in order to battle criminals on an even playing field. Law enforcement already has access to post-cut-through digits by obtaining a warrant under Title III, so denying law enforcement agencies access to post-cut-through digits under CALEA does not impede their ability to investigate crimes. The important issue, however, is whether law enforcement was given special access rights under CALEA, or if law enforcement must rely on its remedies available under Title III and the Fourth Amendment. It is clear that CALEA was meant to preserve law enforcement's access rights, not enhance them. DoJ/FBI's arguments must be rejected.

III. THE COMMISSION'S DECISION TO FORECLOSE COMMENT ON "UNCONTESTED" ISSUES IMPROPERLY INSULATES THE LAW ENFORCEMENT-INDUSTRY STANDARD FROM PUBLIC SCRUTINY.

As EPIC, EFF and ACLU pointed out in initial comments on the DoJ/FBI Petition, public interest organizations dedicated to upholding the public's right to privacy did not have an effective voice in the proceedings that led up to the J-STD-025 standard and the FBI's "punchlist"[86] As the Commission apparently recognizes,[87] law enforcement organizations and the telecommunications industry had extensive meetings to agree on a standard and organizations representing the public were excluded from these meetings. Remarkably, the Commission has chosen to compound that clear error rather than resolve it.

In the *Further Notice*, the Commission makes the apparently final decision that it "do[es] not intend to reexamine any of the uncontested technical requirements of the J-STD-025

Secrecy of Wiretaps," New York Times, 28 (Aug. 2, 1998); Marc Cooper, "Wired," New Times of Los Angeles (Aug. 13, 1998).

86 *See* EPIC/EFF/ACLU Comments, CC Docket 97-213, at 28-29 (May 20, 1998).

87 *See Further Notice* at 23, n.81.

standard."[88] The determination of what elements are "uncontested" apparently has been made by reference to comments filed on the DoJ/FBI Petition. The decision to foreclose public participation by an administrative agency is remarkable at any point, but particularly so at the point of *commencing* a rulemaking proceeding in a *notice of proposed rulemaking* rather than a final order. The Commission's determination that it will not issue a traditional notice of proposed rulemaking explaining the standard it proposes to approve and seeking public comment on that standard – and, indeed, foreclosing any comment by any member of the public on elements of the standard that were not "contested" when petitions for rulemaking were filed – ensures that the public will have no opportunity to be effectively apprised of the contents of the standard that will determine the wiretap functions that will be built into the Nation's telecommunications system. Narrowly, making a final decision of this scope in a notice of proposed rulemaking is inconsistent with the Administrate Procedure Act; broadly, foreclosing discussion of a standard arrived at solely by industry and law enforcement undermines the value of the Commission's overall authority over the process that has led to that standard.

The Commission further gives short shrift to our request that it review the issues in the J-STD-025 standard and the punchlist *de novo*, apparently finding that the ability to cast a ballot on the proposed standard absolved industry and law enforcement of any responsibility to permit public participation in the process leading up to the adoption of the standard.[89] Of course, having the opportunity to cast a ballot after being foreclosed from participating in months-long technical discussions and negotiations is an entirely ineffective substitute for the opportunity to participate fully. The right to vote without the corresponding ability to obtain the critical information on

---

88 *Further Notice* at 23.

which a ballot will be cast is meaningless. Because of the complexity of the technical issues and the societal importance of the decisions to be made, the Commission should have commenced a rulemaking proceeding to investigate these issues *de novo* rather than compound the closed nature of the process by refusing comment on the "uncontested" elements of the law-enforcement/industry standard.[90]

---

89 *See Further Notice* at 23 n.81 (noting that EPIC/EFF/ACLU "have not claimed that they were precluded from participating in the open ANSI balloting process").

90 Having been excluded from the proceedings that produced the interim standard, it is difficult for EPIC/EFF/ACLU to identify with particularity all aspects of the interim standard that implicate privacy considerations. For this reason, the Commission should ensure that *all* of the capability standards that it adopts pursuant to CALEA are done through full notice and comment rulemaking to give all interests an opportunity to heard.

IV. CONCLUSION

For all of the foregoing reasons, we urge the Commission to reject the industry standard and the FBI punchlist proposals and to exercise its duty under CALEA to protect the individual privacy that is a vital component of our Nation's foundation.

Respectfully submitted,

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.
Shari Steele, Esq.
ELECTRONIC FRONTIER FOUNDATION
1550 Bryant Street
Suite 725
San Francisco, California 94103

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

Kurt A. Wimmer
Alane C. Weixel
Mark E. Porada

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 Jeannie Anna Court
Oak Hill, Virginia 20171

December 14, 1998