

IN THE  
UNITED STATES COURT OF APPEALS  
FOR THE DISTRICT OF COLUMBIA CIRCUIT

---

Nos. 99-1442, 99-1466, 99-1475, 99-1523

---

UNITED STATES TELECOM ASSOCIATION,  
CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION,  
CENTER FOR DEMOCRACY AND TECHNOLOGY, *et al.*,

*Petitioners,*

v.

FEDERAL COMMUNICATIONS COMMISSION  
and UNITED STATES OF AMERICA,

*Respondents.*

---

ON PETITION FOR REVIEW OF AN ORDER OF  
THE FEDERAL COMMUNICATIONS COMMISSION

---

BRIEF OF PETITIONERS UNITED STATES TELECOM ASSOCIATION,  
CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION, AND  
CENTER FOR DEMOCRACY AND TECHNOLOGY

---

Theodore B. Olson  
Eugene Scalia  
Montgomery N. Kosma  
GIBSON, DUNN & CRUTCHER LLP  
1050 Connecticut Avenue NW  
Washington, D.C. 20036-5303  
(202) 955-8500

*Counsel for Cellular Telecommunications  
Industry Association and Center for Democracy  
and Technology*

John H. Harwood II  
Lynn R. Charytan  
Samir Jain  
WILMER, CUTLER & PICKERING  
2445 M Street NW  
Washington, D.C. 20037  
(202) 663-6000

*Counsel for United States Telecom  
Association*

(additional counsel listed on inside cover)

January 20, 2000

---

Michael Altschul  
Cellular Telecommunications Industry Association  
1250 Connecticut Avenue NW, Suite 800  
Washington, D.C. 20036  
(202) 785-0081

Jerry Berman  
James X. Dempsey  
Center for Democracy and Technology  
1634 Eye Street NW, Suite 1100  
Washington, D.C. 20006  
(202) 637-9800

Lawrence E. Sarjeant  
Linda L. Kent  
Keith Townsend  
John W. Hunter  
Julie E. Rones  
United States Telecom Association  
1401 H Street, Suite 600  
Washington, D.C. 20036  
(202) 326-7248

## **CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES**

Pursuant to Circuit Rule 28(a)(1), petitioners United States Telecom Association (“USTA”), Cellular Telecommunications Industry Association (“CTIA”), and the Center for Democracy and Technology (“CDT”) submit the following information:

(A) Parties and Intervenors

Petitioner USTA is a non-profit trade association representing the interests of facilities-based local exchange and exchange access providers. Its members also include international members who provide local exchange services in other jurisdictions, and associate members who are consultants, manufacturers, banks and investors, and other parties with interest in the local exchange industry. USTA has no parent companies, subsidiaries, or affiliates for whom disclosure is required by Rule 26.1.

Petitioner CTIA has no parent companies, subsidiaries, or affiliates that have issued shares or debt securities to the public. CTIA is organized as a not-for-profit corporation under the laws of the District of Columbia. CTIA is the international organization of the wireless communications industry for both wireless carriers and manufacturers. Membership in the association covers all Commercial Mobile Radio Service (“CMRS”) providers, and includes 28 of the 30 largest cellular, broadband, and PCS providers. CTIA represents more broadband PCS carriers, and more cellular carriers, than any other trade association.

Petitioner CDT has no parent companies, subsidiaries or affiliates that have issued shares to the public, nor does any publicly-held company hold any ownership interest in CDT. CDT is a 501(c)(3) non-profit, public interest organization incorporated in the District of Columbia, working to defend and enhance privacy protections for new communications technologies.

The Electronic Privacy Information Center, the American Civil Liberties Union, and the Electronic Frontier Foundation are also petitioners in this action.

The respondents in this action are the Federal Communications Commission and the United States of America.

The following parties have intervened in this action: AirTouch Communications, Inc., the Personal Communications Industry Association, the Rural Cellular Association, Sprint Spectrum, L.P., the Telecommunications Industry Association, and U S WEST, Inc.

(B) Ruling under Review

USTA, CTIA, and CDT have petitioned the Court to review the Third Report and Order adopted by the Federal Communications Commission, *In the Matter of Communications Assistance for Law Enforcement Act*, 14 FCC Rcd 16794 (1999). The Order was released on August 31, 1999. A summary of the Order was published in the Federal Register on September 24, 1999. *See* 64 Fed. Reg. 51710. A copy of the Order is contained in an addendum bound with this brief and appears in the Joint Appendix at \_\_\_\_.

(C) Related Cases

This case has not previously been before this Court or any other court. Petitioners USTA, CTIA, and CDT are not aware of any related cases pending in this Court or any other court.

## **TABLE OF CONTENTS**

## **TABLE OF AUTHORITIES**

\* Authorities chiefly relied upon are marked with asterisks.

## **GLOSSARY**

<b>ACLU:</b>	American Civil Liberties Union
<b>CALEA:</b>	Communications Assistance for Law Enforcement Act
<b>CDT:</b>	Center for Democracy and Technology
<b>CTIA:</b>	Cellular Telecommunications Industry Association
<b>DOJ:</b>	Department of Justice
<b>ECPA:</b>	Electronic Communications Privacy Act
<b>EFF:</b>	Electronic Frontier Foundation
<b>EPIC:</b>	Electronic Privacy Information Center
<b>FBI:</b>	Federal Bureau of Investigation
<b>FCC:</b>	Federal Communications Commission
<b>TIA:</b>	Telecommunications Industry Association
<b>USTA:</b>	United States Telecom Association

ORAL ARGUMENT SCHEDULED FOR MAY 17, 2000

IN THE  
UNITED STATES COURT OF APPEALS  
FOR THE DISTRICT OF COLUMBIA CIRCUIT

---

Nos. 99-1442, 99-1466, 99-1475, 99-1523

---

UNITED STATES TELECOM ASSOCIATION,  
CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION,  
CENTER FOR DEMOCRACY AND TECHNOLOGY, *et al.*,

*Petitioners,*

v.

FEDERAL COMMUNICATIONS COMMISSION  
and UNITED STATES OF AMERICA,

*Respondents.*

---

ON PETITION FOR REVIEW OF AN ORDER OF  
THE FEDERAL COMMUNICATIONS COMMISSION

---

BRIEF OF PETITIONERS UNITED STATES TELECOM ASSOCIATION,  
CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION, AND  
CENTER FOR DEMOCRACY AND TECHNOLOGY

---

**JURISDICTIONAL STATEMENT**

These consolidated petitions seek review of a final order of the Federal Communications Commission (“FCC”), *In the Matter of Communications Assistance for Law Enforcement Act*, Third Report and Order, 14 FCC Rcd 16794 (1999) (the “Order”). The Order was released on August 31, 1999. A summary of the Order was published in the Federal Register on September 24, 1999. *See* 64 Fed. Reg. 51710. A copy of the Order is contained in an addendum bound with this brief and appears in the Joint Appendix at \_\_\_\_.

Petitioner USTA timely filed its petition for review on November 9, 1999, and CTIA and CDT timely petitioned for review on November 22, 1999. This Court therefore has jurisdiction pursuant to 47 U.S.C. § 402(a) and 28 U.S.C. § 2342(1). Venue lies in this Court pursuant to 28 U.S.C. § 2343.

### **STATEMENT OF ISSUES PRESENTED FOR REVIEW**

1. Whether the FCC violated the plain meaning of the Communications Assistance for Law Enforcement Act (“CALEA”), 47 U.S.C. § 1001 *et seq.*, and otherwise acted arbitrarily and capriciously when it determined that information about the physical location of a caller using a mobile telephone, and information provided by certain electronic surveillance capabilities requested by the FBI, constitute “call-identifying information reasonably available to the carrier” and therefore must be provided by carriers to law enforcement.

2. Whether the FCC’s failure to consider CALEA’s explicit criteria for imposing capabilities on carriers violated the statute and was arbitrary and capricious.

3. Whether the FCC’s decision to require carriers to develop a capability to deliver “packet” communications to law enforcement agencies (a) was arbitrary and capricious in light of the agency’s concession that the record was deficient on the issue, and (b) exceeded the FCC’s authority under CALEA by imposing – yet admitting it may later retract – a requirement that would result in government interception of communications in violation of the Fourth Amendment and Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. § 2510 *et seq.*

### **RELEVANT STATUTORY PROVISIONS AND REGULATIONS**

Pertinent statutory provisions and regulations are set forth in an addendum bound with this brief.

## JOINT STATEMENT OF THE CASE

Petitioners United States Telecom Association (“USTA”), Cellular Telecommunications Industry Association (“CTIA”), Center for Democracy and Technology (“CDT”), American Civil Liberties Union, Electronic Frontier Foundation, and Electronic Privacy Information Center challenge key portions of an Order of the Federal Communications Commission (“FCC”) imposing obligations on telecommunications carriers to provide support for electronic surveillance under the Communications Assistance for Law Enforcement Act (“CALEA”), 47 U.S.C. § 1001 *et seq.* CALEA requires carriers to take steps to ensure that technological advances do not preclude law enforcement agencies from obtaining information to which they may be entitled under certain laws authorizing limited electronic surveillance. CALEA is the product of a careful congressional balancing of the interests of law enforcement and the equally important national policies of protecting individual privacy, minimizing costs to consumers and suppliers of telecommunications services, and encouraging the continuing development of new communications technologies and services.

The FCC’s Order implementing CALEA upsets this fragile balance. It imposes requirements that violate the plain meaning of CALEA and that, contrary to Congress’s stated purpose, will result in considerable intrusions on personal privacy, increased communications costs, and barriers to technological innovation. The FCC failed to satisfy even minimal standards of reasoned decisionmaking and drew conclusions based on little more than agency *ipse dixit*. In so doing, the FCC unlawfully required carriers to enable law enforcement to obtain information outside the scope of CALEA, such as the location of mobile telephone users and the content of private electronic communications in certain circumstances where law

enforcement lacks the requisite court order to access content information. The petitioners accordingly request that this Court vacate as arbitrary, capricious, and contrary to law the portions of the FCC’s Order discussed below.

## **JOINT STATEMENT OF FACTS**

### **A. Statutory Background**

#### *1. Electronic Surveillance*

CALEA was enacted within the context of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. § 2510 *et seq.* (“Title III”), and the pen register and trap and trace provisions of the Electronic Communications Privacy Act of 1986 (“ECPA”), 18 U.S.C. § 3121 *et seq.* Motivated principally by concerns over privacy rights, these statutes articulate broad federal prohibitions against wiretapping or eavesdropping on communications. They establish procedures to enable law enforcement to conduct electronic surveillance only in two carefully confined, court-approved circumstances: (i) intercepting the *contents* of communications and (ii) obtaining the *telephone numbers* to which a person makes calls and from which the person receives calls.

Title III governs the interception of the “contents” of communications, which the statute defines as “any information concerning the substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(8). “Animating the whole of Title III [was] ‘an overriding congressional concern’ with the protection of individual privacy.” *Lam Lek Chong v. U.S. Drug Enforcement Admin.*, 929 F.2d 729, 732 (D.C. Cir. 1991) (quoting *Gelbard v. United States*, 408 U.S. 41, 48 (1972)). Title III accordingly imposes strict limitations on the ability of law enforcement to obtain call content – limitations that embody, and in some respects go beyond, the protections guaranteed by the Fourth Amendment. Absent exigent circumstances, a law

enforcement agency may intercept content only pursuant to a court order issued upon findings of probable cause to believe that an individual is committing one of a list of specifically enumerated crimes, that communications concerning the specified offense will be intercepted, and that the pertinent facilities are commonly used by the alleged offender or are being used in connection with the offense. 18 U.S.C. § 2518(3).

ECPA establishes minimum standards for court-approved law enforcement access to the “electronic or other impulses” that identify “the numbers dialed” for outgoing calls and “the originating number” for incoming calls. 18 U.S.C. §§ 3127(3)-(4). This narrow category of information is not protected by the Fourth Amendment. *Smith v. Maryland*, 442 U.S. 735, 742 (1979). ECPA nevertheless requires law enforcement agencies to obtain a court order before using a “pen register” for outgoing calls or a “trap and trace” device for incoming calls. To obtain such an order, the government need merely certify that “the information likely to be obtained is relevant to an ongoing criminal investigation.” 18 U.S.C. §§ 3122-23.

Neither Title III nor ECPA authorizes law enforcement to obtain any other information.

## 2. *Origins and Purpose of CALEA*

CALEA grew out of concerns that advances in telecommunications technology had begun to outpace law enforcement’s ability to obtain information to which it was entitled under Title III and ECPA. As FBI Director Louis Freeh testified, “[t]he purpose of this legislation, quite simply, is to *maintain* technological capabilities commensurate with existing statutory authority – that is, to prevent advanced telecommunications technology from repealing, de facto, statutory authority now existing and conferred to us by the Congress.” *Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearings on H.R. 4922 and S. 2375*, 103d Cong. 7 (1994) (“Joint Hearings”) (emphasis added).

CALEA was thus enacted to “*preserve* the government’s ability . . . to intercept communications involving advanced technologies such as digital or wireless transmission.” H.R. Rep. No. 103-827, at 9 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489 (“House Rep.”) (emphasis added). Director Freeh was emphatic that law enforcement was “not seeking any expansion of the authority Congress gave to law enforcement when the wiretapping law was enacted 25 years ago.” Joint Hearings at 6. Congress explicitly adopted this principle, stating that CALEA “will not expand” statutory authority to conduct electronic surveillance because it is “intended to preserve the status quo . . . to provide law enforcement no more and no less access to information than it had in the past.” House Rep. at 17, 22; *see also* Joint Hearings at 32 (CALEA “ensures a maintenance of the status quo . . . as it relates to the types of information obtainable through pen register and trap and trace devices.”). The scope of CALEA’s requirements is thus confined to preserving law enforcement’s ability to obtain information under Title III and ECPA.

CALEA’s scope is further limited by other important national policies. As the House Report explained, CALEA was intended not only “to preserve a narrowly focused capability . . . to carry out properly authorized intercepts,” but also “to protect privacy in the face of increasingly powerful and personally revealing technologies; and . . . to avoid impeding the development of new communications services and technologies.” House Rep. at 13. Congress took steps to minimize the costs to taxpayers, consumers, and the industry, and to prevent law enforcement from “goldplating” the capabilities required under CALEA. *Id.* at 49. It required the federal government to “pay carriers for just and reasonable costs incurred in modifying existing equipment, services or features to comply with the capability requirements” and provided that any particular requirements imposed on industry must be cost effective. *Id.* at 10; *see* 47 U.S.C. §§ 1008, 1006(b)(1).

To preserve the delicate balance struck by CALEA, Congress admonished against “overbroad interpretation of the [statutory] requirements” and explained that it “expect[ed] industry, law enforcement and the FCC to *narrowly interpret [CALEA’s] requirements.*” House Rep. at 22-23 (emphasis added).

### 3. *Statutory Framework*

CALEA imposes carefully circumscribed duties on carriers to retrofit or design their networks so that law enforcement can conduct lawful electronic surveillance:

- To allow interception of *call contents* under Title III, carriers must “enabl[e] the government, pursuant to a court order or other lawful authorization, to intercept . . . all [a subscriber’s] wire and electronic communications carried by the carrier.” *Id.* § 1002(a)(1).
- To permit monitoring of *numbers dialed* under ECPA, carriers must “enabl[e] the government, pursuant to a court order or other lawful authorization, to access *call-identifying information* that is *reasonably available* to the carrier.” *Id.* § 1002(a)(2) (emphasis added).
- Carriers must ensure that authorized interceptions are conducted “unobtrusively and . . . in a manner that protects the privacy and security of communications and call-identifying information not authorized to be intercepted.” 47 U.S.C. § 1002(a)(4).<sup>1</sup>

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.” *Id.* § 1001(2). The Act expressly excludes location information, providing that, where law enforcement has authorization only for a pen register or trap and trace device under ECPA, “call-identifying information shall *not* include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number).” *Id.* § 1002(a)(2) (emphasis added).

---

<sup>1</sup> Although not at issue here, CALEA also establishes requirements for delivery of information to the government. 47 U.S.C. § 1002(a)(3).

CALEA authorizes industry standard-setting associations to formulate technical requirements for compliance. A carrier is deemed in compliance with CALEA if it adheres to an industry standard – a “safe harbor.” *Id.* § 1006(a). Law enforcement’s role in the standards process is limited to “consult[ation] with appropriate associations and standard-setting organizations”; it may not require or prohibit “any specific design” of equipment, facilities, services, features, or system configurations. *Id.* §§ 1002(b), 1006(a).

CALEA empowers the FCC to modify an industry standard on petition by any agency or person claiming that the standard is “deficient.” 47 U.S.C. § 1006(b). The FCC may add or modify a requirement only if the new requirement (i) meets the statutory capability requirements by cost-effective methods, (ii) protects the privacy and security of communications not authorized to be intercepted, (iii) minimizes the costs of such compliance on residential ratepayers, (iv) encourages the provision of new technologies and services, and (v) provides reasonable time and conditions for compliance. *Id.*

## **B. Industry Standard and FCC Proceedings**

### *1. Development of Industry Standard*

Carriers and telecommunications equipment manufacturers began working to develop a safe harbor standard in early 1995 through two standard-setting committees accredited by the American National Standards Institute (“ANSI”). In 1996, the FBI set forth an expansive list of features it wanted carriers to implement and the specific technical means by which they should be provided. The industry published a standard that included all the features mandated by the language of CALEA or mentioned in the legislative proceedings, as well as some concessions to the FBI demands. The standard – the Interim Standard/Trial Use Standard J-STD-025 or “J-Standard” – was adopted by industry in December 1997. (J.A. \_\_-\_\_.)

## 2. *Proceedings before the FCC*

On March 27, 1998, the FBI petitioned the FCC to add what it called a “punch list” of nine capabilities to the J-Standard. Department of Justice/FBI Joint Petition for Expedited Rulemaking (Mar. 27, 1998) (“DOJ/FBI Petition”). (J.A. \_\_\_-\_\_\_.) Petitioner CDT also challenged the J-Standard as exceeding CALEA’s capability requirements and violating the statute’s mandate to protect the privacy of communications not authorized to be intercepted. CDT argued that the standard improperly required carriers to provide information about the physical location of mobile telephone users and permitted law enforcement to intercept the content of “packet-mode” communications without the requisite Title III authorization. CDT Petition for Rulemaking under Sections 107 and 109 of CALEA (Mar. 26, 1998). (J.A. \_\_\_-\_\_\_.)

The FCC sought public comment on the deficiency petitions on April 20, 1998, and again in a Further Notice of Proposed Rulemaking issued November 5, 1998. 13 FCC Rcd 22632 (1998) (“Further NPRM”). (J.A. \_\_\_-\_\_\_.) The FCC released its Order on August 31, 1999.

**Call-Identifying Information.** The FCC concluded that the cell site location of a person’s mobile telephone is “call-identifying information” and required that carriers report that information at the beginning and end of each call. Order ¶¶ 44-46. The FCC also concluded that four of the capabilities demanded by the FBI meet CALEA’s definition of “call-identifying information” and are “reasonably available” to carriers, and accordingly required carriers to implement them. The four added capabilities are:

- “Dialed digit extraction” – Information about any digits dialed by a telephone being monitored under a pen register *after* a call has been connected (*e.g.*, bank account or credit card numbers, as well as phone numbers entered after calling a long distance provider). *Id.* ¶¶ 119-23.
- “Party hold/join/drop” – Information indicating when a party on a multi-party conference call is on hold, has joined, or has dropped from the call. *Id.* ¶¶ 74-75.

- “Subject-initiated dialing and signaling” – Information about a person’s activation or intended use of features such as call waiting and call forwarding. *Id.* ¶ 82.
- “In-band and out-of-band signaling” – Information about any network message sent to a monitored telephone (such as ringing, a call waiting signal, or a message light). *Id.* ¶ 89.

The FCC did not attempt to define the terms used in the definition of “call-identifying information” (i.e., origin, direction, destination, and termination).

The FCC stated that cost is a significant factor in determining whether call-identifying information is “reasonably available.” Order ¶¶ 29-30. It accepted as a “guide” the estimates provided by a few equipment manufacturers for the revenues they expected to earn from sales of CALEA-compliant software to carriers: \$916 million for the J-Standard and \$414 million for the added capabilities demanded by the FBI. *Id.* ¶ 30. But the FCC did not articulate any criteria for taking cost into account, nor did it explain when costs would be too high to meet the “reasonably available” requirement. Instead, it simply asserted, repeatedly, that the costs it was imposing were “not so exorbitant.” *Id.* ¶¶ 30, 66, 75, 82, 89, 95, 123.

The Order also did not analyze whether location information or the four added capabilities satisfy the five criteria that, under CALEA, must be met before any requirements are added to an industry standard. 47 U.S.C. § 1006(b).<sup>2</sup>

**Packet-Mode Communications.** The FCC acknowledged that the J-Standard would permit law enforcement agencies to receive the contents of packet communications even when the agencies are not authorized under Title III or other pertinent authority to obtain call content. Order ¶ 56. USTA, the Telecommunications Industry Association (“TIA”), and other industry commenters had explained that separating call-identifying information from the packet’s content

---

<sup>2</sup> The FCC rejected three of the FBI’s punch list items, Order ¶¶ 101, 106, 111, and accepted two others in modified form, *id.* ¶¶ 64-67, 95-96. Those rulings are not challenged in this petition.

is not feasible and would slow, if not stifle, the development of packet-based technologies. Comments of USTA at 11-13 (Dec. 14, 1998); Comments of TIA at 44 (Dec. 14, 1998). (J.A. \_\_\_-\_\_\_.) The FCC concluded that the record did not “sufficiently address[] packet technologies and the problems that they may present for CALEA purposes.” Order ¶ 55. It accordingly “invite[d]” TIA “to study CALEA solutions for packet-mode technology and report to the Commission in one year on steps that can be taken, including particular amendments to [the J-Standard], that will better address privacy concerns.” *Id.* Notwithstanding these findings, the FCC ordered carriers to deliver packets to law enforcement in the interim, even though that would result in law enforcement “receiv[ing] . . . call content under a pen register.” *Id.* ¶ 56.

### **SUMMARY OF ARGUMENT**

The FCC improperly extended CALEA to capture a broad range of private information based on little more than agency *ipse dixit* and without meaningful analysis of the statute’s terms. As a result, its Order conflicts with the plain meaning and purpose of CALEA and the federal wiretap laws in three principal respects.

First, CALEA and the wiretap laws make clear that “call-identifying information” refers only to the telephone numbers used to route calls. The Order misconstrues this term to effect a significant and unauthorized invasion of citizens’ privacy by converting cellular telephones into location tracking devices. FBI Director Louis Freeh explicitly disclaimed any intention to use CALEA to expand the power of law enforcement or to obtain the location of persons making telephone calls, but the Order breaches both of these barriers.

Second, the FCC further misinterpreted the term “call-identifying information” to adopt four of the additional capabilities demanded by the FBI. The Order requires telephone carriers to supply law enforcement agencies, acting without Title III authority, credit card and bank account

numbers and other signals in excess of the telephone numbers authorized by CALEA and ECPA. In improperly expanding law enforcement authority in this manner, the agency disregarded CALEA's explicit statutory commands to protect privacy, encourage innovation, and avoid unwarranted costs to industry and consumers.

Third, the FCC required carriers to supply law enforcement with the contents of digital packet communications while simultaneously acknowledging that the record was insufficient to decide the issue and ordering further studies of the subject. The packet order will result in violations of Title III and the Fourth Amendment by requiring carriers to give the content of telephone calls to law enforcement authorities who lack the necessary court order.

### **ARGUMENT**

The FCC's Order implementing CALEA must be set aside because it conflicts with the Act's plain meaning as determined by "traditional tools of statutory construction." *See Chevron U.S.A. Inc. v. Natural Resources Defense Council, Inc.*, 467 U.S. 837, 842-43 & n.9 (1984). Under *Chevron*, the first inquiry is "whether Congress has directly spoken to the precise question at issue." *Id.* at 842. Conducting this inquiry requires "examination of the statute's text, legislative history, and structure, as well as its purpose." *Bell Atlantic Tel. Cos. v. FCC*, 131 F.3d 1044, 1047 (D.C. Cir. 1997) (citations omitted). "If this search yields a clear result, then Congress has expressed its intention as to the question, and deference [to the agency's resolution of the question] is not appropriate." *Id.*; *see also Panamsat Corp. v. Federal Communications Commission*, No. 98-1408, 1999 WL 1215311 at \*6 (D.C. Cir. Dec. 21, 1999) (no deference is due to an agency's "erroneous interpretation of law") (citation omitted).

Even if CALEA were deemed ambiguous and the second step of *Chevron* applied, deference still would be inappropriate because the Order does not articulate any affirmative

interpretation of the statutory language to which this Court could defer. 467 U.S. at 842-43. As this Court has held, a court “cannot defer to a vacuum,” *Colorado Interstate Gas Co. v. FERC*, 850 F.2d 769, 774 (D.C. Cir. 1988), or “to mere decisional evasion.” *Competitive Enter. Inst. v. NHTSA*, 956 F.2d 321, 323 (D.C. Cir. 1992); *see also Achernar Broad. Co. v. FCC*, 62 F.3d 1441, 1447 (D.C. Cir. 1995) (“While agency expertise deserves deference, it deserves deference only when it is exercised.”).

Moreover, the FCC’s interpretation of CALEA’s capability requirements is not entitled to deference because determining the scope of those requirements necessitates interpreting Title III and ECPA, but Congress has not delegated to the FCC the authority to do so. Where Congress has not delegated interpretive authority to the agency, courts “engage in a *de novo* interpretation of the statute, guided, of course, by Congressional intent.” *Professional Airways Sys. Specialists v. Federal Labor Relations Auth.*, 809 F.2d 855, 857 n.6 (D.C. Cir. 1987).

**I. THE FCC WRONGLY CONCLUDED THAT LOCATION INFORMATION AND THE FOUR ADDED CAPABILITIES ARE REQUIRED BY CALEA.**

Neither location information nor the information provided by the four challenged capabilities added by the FCC is “call-identifying information” within the meaning of CALEA. 47 U.S.C. § 1002(a)(2). And the FCC failed to articulate or apply reasoned criteria for determining that these capabilities are “reasonably available” to carriers.

**A. “Call-Identifying Information” under CALEA Is Limited to Information Identifying the Numbers Dialed or Transmitted To Route Calls.**

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.” *Id.* § 1001(2). As CALEA’s language and legislative history and the

underlying provisions of Title III and ECPA demonstrate, this definition confines “call-identifying information” to the numbers dialed or transmitted to route calls.

A telephone network “identifies” a call by the telephone numbers used to route it – the numbers of the calling and called parties and, where call forwarding is used, the forwarding and forwarded-to numbers. In the telecommunications industry, these numbers are called “address signals.”<sup>3</sup> The J-Standard defined “call-identifying information” in accordance with this well understood meaning, a definition that the FCC did not even discuss. J-Standard at 5. (J.A. \_\_\_.)

Thus, under the J-Standard, the statutory terms used to define “call-identifying information” correspond to particular telephone numbers. “Origin” is the number of the phone originating a call: this is the identifying information picked up by both “caller ID” and trap and trace devices. “Destination” is the number dialed by a person making an outgoing call: this is the information used to identify calls on long-distance bills and picked up by pen registers. “Direction” is the number to which or from which a call is redirected, a number increasingly important with the advent of call-forwarding, one of the major law enforcement concerns that led to the enactment of CALEA. “Termination” is the number of the phone where the call is ultimately answered. *Id.* Although the destination, direction, and termination will often be the same, they may differ if call-forwarding is used: as a call moves through multiple switches, the number to which the call is directed may differ from the destination dialed by the party originating the call, and the call may be redirected several times before it reaches its termination.

This plain meaning of call-identifying information is confirmed by CALEA’s legislative history. Congress explained that, for voice communications, call-identifying information is

---

<sup>3</sup> See R. Freeman, *Reference Manual for Telecommunications Engineering* 81 (2d ed. 1994); M. Gallagher & R. Snyder, *Mobile Telecommunications Networking* 79 (1997).

“typically the electronic pulses, audio tones, or signalling messages that *identify the numbers dialed or otherwise transmitted for the purpose of routing calls* through the telecommunications carrier’s network.” House Rep. at 21 (emphasis added); *id.* at 16 (call-identifying information is “information identifying the *originating and destination numbers* of targeted communications” (emphasis added)).

These conclusions reflected FBI Director Freeh’s own testimony about the scope of call-identifying information:

Law enforcement’s requirements set forth in the proposed legislation include an ability to acquire “call setup information.” This information relates to dialing type information – information generated by a caller which identifies the origin, duration, and destination of a wire or electronic communication, the telephone number or similar communication address. . . . What I want with respect to pen registers is the dialing information: telephone numbers which are being called, which I have now under pen register authority.

Joint Hearings at 33, 50. No less than ten times during his testimony, Director Freeh described this capability as consisting simply of “dialing information.” *See, e.g., id.* at 24, 27-28.

CALEA’s requirement for call-identifying information corresponds precisely with the information available through pen registers and trap and trace devices under ECPA: pen registers capture “impulses which identify *the numbers dialed or otherwise transmitted*” and trap and trace devices capture “impulses which identify *the originating number* of an instrument or device from which a wire or electronic communication was transmitted.” *See* 18 U.S.C. §§ 3127(3)-(4) (emphasis added). Indeed, CALEA amended ECPA to make clear that an agency using a pen register is authorized to obtain only “dialing and signaling information *utilized in call processing.*” 18 U.S.C. § 3121(c).<sup>4</sup>

---

<sup>4</sup> CALEA’s enforcement provision requires only capabilities to intercept content for Title III and the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.*, and to monitor dialed [footnote continued on following page]

It would have made no sense for Congress to require carriers to provide a capability that the surveillance laws do not authorize the government to use. The Fourth Amendment is inapplicable to pen registers – and law enforcement accordingly need only satisfy a low standard of relevance to use such devices – precisely because the devices do no more than monitor the numbers dialed to connect calls. *See Smith v. Maryland*, 442 U.S. 735, 742 (1979). Thus, interpreting CALEA in light of the definitions and limitations of ECPA confirms the limited understanding of “call-identifying information” adopted by Congress. *See generally Davis v. Michigan Dept. of Treasury*, 489 U.S. 803, 809 (1989) (“[T]he words of a statute must be read in their context and with a view to their place in the overall statutory scheme.”).

**B. The FCC’s Interpretation of “Call-Identifying Information” Conflicts with the Plain Meaning of That Term, Applies the Term Inconsistently, and Lacks a Reasoned Explanation.**

Basic norms of statutory construction required the FCC to give a fixed definition to each of CALEA’s key terms and then apply that definition consistently. Yet the Order nowhere attempts to define the terms “destination,” “direction,” “origin,” or “termination,” or to explain the scope of “call-identifying information.” Nor did the FCC purport to find any deficiency in the J-Standard’s definitions of these terms, or to explain why it believes that “call-identifying information” extends beyond the numbers dialed for routing calls. The *only* FCC discussion of any of these statutory terms is in the context of particular capabilities. But even there the FCC did nothing more than assert without analysis that the information in question identifies the “destination,” “direction,” “origin,” or “termination” of a call. *See infra* at 18-27 (discussing each of the challenged capabilities).

---

number information for ECPA’s pen register and trap and trace provisions. *See* 18 U.S.C. § 2522(a).

It is not enough for an agency simply to recite a party's arguments and then issue "ipse dixit conclusion[s]." *Illinois Pub. Telecomms. Ass'n v. FCC*, 117 F.3d 555, 564 (D.C. Cir. 1997); *see also Building & Constr. Trades Dep't, AFL-CIO v. Martin*, 961 F.2d 269, 277 (D.C. Cir. 1992) ("To state a conclusion is not to reason."). Rather, "'an agency must cogently explain why it has exercised its discretion in a given manner,' and that explanation must be 'sufficient to enable [a court] to conclude that the [agency's action] was the product of reasoned decisionmaking.'" *A.L. Pharma, Inc. v. Shalala*, 62 F.3d 1484, 1491 (D.C. Cir. 1995) (citation omitted) (*quoting Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 28, 48, 52 (1983)). The FCC's Order fails this basic test.

Moreover, the FCC's conclusions that location information and the four categories of information added to the J-Standard constitute "call-identifying information" are contrary to the plain meaning of the statute. The terms "destination," "direction," "origin," and "termination" necessarily must be defined to include telephone numbers so that carriers will provide the information captured by pen registers and trap and trace devices under ECPA. But, as discussed more fully below, location information and the capabilities added by the FCC do not identify phone numbers. Accordingly, the FCC could determine that the information it added is "call-identifying information" only by assuming that the terms "destination," "direction," "origin," and "termination" simultaneously refer *both* to phone numbers and to a variety of other types of information provided by the added capabilities. For example, "origin" must refer to the phone number of the party initiating the call. The FCC ruled, however, that "origin" also means the signal indicating that a call is waiting, Order ¶ 82; use of the flash key on the telephone to switch back and forth between two established calls, *id.*; putting a party on hold, *id.* ¶ 74; and the location of a wireless phone caller at the beginning and end of a call, *id.* ¶ 44.

Assigning such different and expansive meanings to a term violates basic canons of statutory construction. *See Ratzlaf v. United States*, 510 U.S. 135, 143 (1994) (“A term appearing in several places in a statutory text is generally read the same way each time it appears. *We have even stronger cause to construe a single formulation . . . the same way each time it is called into play.*” (emphasis added)). Doing so without a rational explanation compounds the agency’s error.

**C. Location Information Is Not “Call-Identifying Information” Required by CALEA.**

The FCC wrongly required carriers to report a person’s cell-site location at the beginning and end of each wireless telephone call on the theory that location “identifies the ‘origin’ or ‘destination’ of a communication.”<sup>5</sup> Order ¶ 44. Under the Order, law enforcement would receive the location of a mobile phone user in an area as precise as a city block in urban locations every time that person used his telephone – information that would readily yield a picture of a mobile phone user’s movements, his whereabouts at any given time, and the pattern of his business and personal life over the course of days or weeks.

This new and intrusive surveillance capability is not authorized by CALEA. Location information is not within the scope of the existing legal authority that CALEA was intended to preserve, because it is neither content subject to interception under Title III, nor information that can be collected by pen registers and trap and trace devices under ECPA. Director Freeh himself rejected the argument that CALEA would require disclosing location information. Joint

---

<sup>5</sup> Law enforcement initially demanded that wireless carriers provide “continuous information about the location of an intercept subject’s cellular phone” even if the phone is not in use. TIA Petition for Rulemaking, Appendix 2, at 3 (Apr. 2, 1998). (J.A. \_\_\_.) Industry refused because such a capability would “greatly exceed” CALEA’s requirements, and instead included the location capability at issue here, “even though many industry participants felt that even this compromise exceeded the scope of CALEA.” *Id.*

Hearings at 33. And Congress took the extra step of prohibiting carriers that already record location information from delivering it to law enforcement under pen register or trap and trace orders. 47 U.S.C. § 1002(a)(2).

1. *A Wireless Telephone User's Geographic Location Is Not "Call-Identifying Information" under CALEA.*

A mobile telephone user's physical location is not call-identifying information under CALEA for four independent reasons.

First, location is not "dialing or signaling information that *identifies . . . each communication.*" 47 U.S.C. § 1001(2) (emphasis added). A wireless telephone does not transmit its location when it places or receives a call. Rather, the handset periodically registers with the network via the nearest cell site – every ten minutes on average – whenever its power is on, *independent of whether or not a call is being made.*<sup>6</sup> As the FCC stated in rejecting a similar capability demanded by the FBI, such network messages are "used by carriers for supervision or control of certain functions and features of the network and do not trigger any audible or visual message to the subscriber and, thus, would not be call-identifying information." Order ¶ 89.

Second, contrary to the FCC's assertion, location does not identify either "the 'origin' or 'destination' of a communication." Order ¶ 44. As described earlier, these terms refer to the telephone numbers of the calling and called parties – numbers that are used for *call routing*. Thus, the terms refer to the path of the *communication*, not that of the *caller*. See House Rep. at 21 (call-identifying information consists of signals that "identify the numbers dialed or otherwise transmitted *for the purpose of routing calls* through the . . . carrier's network.") (emphasis added); see also, e.g., *Florida Public Telecomm. Ass'n v. FCC*, 54 F.3d 857, 859-60 (D.C. Cir. 1995) (describing telephone numbers as "indicating the final destination of the call"); *Internet*

*Over Cable: Defining the Future In Terms of the Past*, FCC OPP Working Paper No. 30, 1998 WL 567433 at \*33 (Aug. 1998) (defining “destination” as a network address).

Third, interpreting “origin” and “destination” to include location would produce nonsensical and inconsistent definitions. For example, under the FCC’s Order, a call placed by a person driving a car would have three “origins”: the caller’s phone number, his geographic location when the call was made, and his geographic location when the call ended. A subject receiving a call on a wireless phone would similarly register up to three “destinations.” The FCC’s definitions inexplicably change, however, when a person who is not an intercept subject uses a mobile phone to call the subject. In that event, only the caller’s phone number – *not* his location – is the call’s “origin.” And when the subject calls someone else’s mobile phone, only the recipient’s phone number – and again, not his location – is the call’s “destination.” These shifting definitions are irrational and depend only on what information law enforcement desires. They have no basis in the language of CALEA, and the FCC offered no rationale for them.

Fourth, the physical location of a mobile caller is precisely the sort of personal information the FBI and Congress repeatedly indicated was not to be authorized by CALEA. For example, Director Freeh testified that the Act would not cover “any information that may disclose the physical location of a mobile facility or service beyond that associated with the number’s area code or exchange.” Joint Hearings at 33; *see also id.* at 114, 116. The House report explained that carriers must provide “information identifying the originating and destination numbers of targeted communications, but *not the physical location of targets.*” House Rep. at 16 (emphasis added). If Congress had meant CALEA to include location, it could have easily used the term. It plainly had no such intention.

---

<sup>6</sup> See Freeman, *supra* note 3, at 1198-99; Gallagher & Snyder, *supra* note 3, at 162-63, 168-77.

2. *Mandating the Implementation of Location Reporting Would Impermissibly Expand Government's Electronic Surveillance Capabilities.*

The FCC's Order significantly expands government's electronic surveillance capabilities, violating CALEA's mandate to do no more than preserve existing authority under Title III and ECPA. Those statutes authorize interception of call content and monitoring of dialed-number information. Neither authorizes law enforcement officials to monitor a person's location in near real-time.

The FCC's interpretation of call-identifying information to include location also presents constitutional difficulties. The Fourth Amendment does not apply to using pen registers to monitor the telephone numbers a person calls, but location monitoring does in some circumstances implicate the Fourth Amendment. *Smith v. Maryland*, 442 U.S. at 742; *United States v. Karo*, 468 U.S. 705 (1984). The FCC wholly ignored these constitutional implications.

3. *The FCC Wrongly Concluded That Congress Designed CALEA To Include Location.*

The FCC attempted to justify its decision on the basis of language in CALEA that expressly *prohibits* carriers from delivering location information to government officials operating "solely pursuant to the authority for pen registers and trap and trace devices." 47 U.S.C. § 1002(a)(2). The FCC suggested that this provision would be "mere surplusage" unless CALEA imposed a mandate to provide location information under some other (unidentified) authority. Order ¶ 44 n.95. But this conclusion ignores Congress's explanation that this prohibition was necessary because location was already available in some systems, independent of CALEA's requirements. House Rep. at 17. Precisely because of this concern, Director Freeh recommended adding language to make it explicit that location could not be obtained through a pen register. Joint Hearings at 33. The prohibition in section 1002(a)(2) was

added for this purpose, as he acknowledged in his subsequent August 1994 testimony. *Id.* at 114, 116. Director Freeh never suggested that CALEA required or should be modified to require the location capability under any other circumstances. And, one day before CALEA was enacted, Congress reiterated its understanding that call-identifying information excluded location, and highlighted this provision as a privacy enhancement. House Rep. at 16-17. Thus, the FCC’s reliance on this provision as a justification to intrude on privacy contradicts its very purpose.

**D. The Four Capabilities Added by the FCC Are Not “Call-Identifying Information” Required by CALEA.**

*1. Dialed Digit Extraction*

“Dialed digit extraction” requires carriers to provide law enforcement with all of the numbers dialed by the intercept subject after a call has been connected. Order ¶ 112. These “post-cut-through digits” fall into two categories: (i) digits specifying credit card numbers, bank account numbers, voicemail passwords or commands, and other information a caller dials after connecting, for example, to a bank or other business; and (ii) digits representing the phone number of the ultimate recipient of the call when the customer has first called an 800 number to reach a long distance carrier.

The FCC admitted that digits falling in the first category are content, *not* call identifying information. Order ¶ 119. For example, the account number of a customer calling a bank to access credit card or account information has nothing to do with the origin, destination, termination, or direction of the call. The account number is part of the *content* of the call, fully protected under the Fourth Amendment and the stringent standards of Title III. The FCC nevertheless required carriers to provide law enforcement all post-cut-through digits as part of the delivery of call-identifying information under only a pen register authorization. *Id.* ¶ 123.

The FCC's purpose in expanding the pen register authority was to enable law enforcement to capture the second category of post-cut-through digits, the telephone number a caller dials after using an 800 number to reach a long distance carrier. But that rationale cannot justify requiring this unlawful disclosure of content. *See Brown v. Waddell*, 50 F.3d 285 (4th Cir. 1995) (holding that "clone" pager devices cannot be authorized under pen register authority because, even though they typically display telephone numbers, some of the digits intercepted may be a communication's content).

In any event, even the numbers dialed after reaching a long distance carrier are not "call-identifying information." From the local carrier's perspective, all post-cut-through digits are *content*. Once a caller has dialed an 800 number, the local carrier has no way of knowing what any subsequent digits represent – an account number, a voicemail password, or a telephone number – and certainly does not use the digits for purposes of call processing. *See* 18 U.S.C. § 3121(c) (pen registers limited to collection of "information *utilized in call processing*" (emphasis added)). Call-identifying information consists of "the numbers dialed or otherwise transmitted for the purpose of *routing calls through the telecommunications carrier's network*," *not* through the network of *another* carrier. House Rep. at 21 (emphasis added).

The Order is all the more arbitrary because law enforcement can obtain post-cut-through call-routing digits by at least two alternative means that avoid the statutory and constitutional problems created by the Order. Law enforcement can obtain a Title III order entitling it to intercept the contents of the subject's call, which would include any post-cut-through digits. Or, because post-cut-through dialed digits do constitute call-identifying information from the standpoint of the long distance carrier, law enforcement may obtain those dialed digits by directing a pen register order to that provider. While the FCC asserted that these alternatives

might be less convenient or more costly for law enforcement, Order ¶¶ 120-21, CALEA was “not intended to guarantee ‘one-stop shopping’ for law enforcement.” House Rep. at 22.

## 2. *Party Hold/Join/Drop on Conference Calls*

This capability requires carriers to send a message to law enforcement whenever a party to a conference call is placed on hold, drops off the call, or joins the call (e.g., by being taken off hold). Order ¶ 68. The FCC’s *entire* explanation for its position that this information falls within the definition of “call-identifying information” consists of the statement that “[p]arty join information *appears* to identify the origin of a communication; party drop, the termination of a communication; and party hold, the temporary origin, temporary termination, or re-direction of a communication.” *Id.* ¶ 74 (emphasis added). That “analysis” – which permits the FCC to rest on its unvarnished assertion that the information at issue “appears” to be call-identifying information – falls far short of reasoned decisionmaking.

Information about whom a subscriber puts on hold does not “identify the numbers dialed or otherwise transmitted for the purpose of routing calls.” House Rep. at 21. A multi-party call is identified by the phone number of each participant, and the J-Standard provides each of these numbers. Once a conference call is established, the origin, direction, destination, and termination of that call are fixed. Putting a party on hold and then adding him back to the call does not require dialing any additional numbers or alter any of those attributes of the call. And, as discussed above, since the “origin” of a communication is the phone number of the party initiating the conference call, it cannot simultaneously mean the time a party re-joins a call after being on hold.

The FBI’s own justification for demanding this capability highlights why the capability exceeds law enforcement’s statutory authority under ECPA. The FBI sought this capability so it could identify the parties on a call at any given time. DOJ/FBI Petition at 75 (J.A. \_\_\_.) But

“[n]either the purport of any communication between the caller and the recipient of the call, *their identities*, nor whether the call was even completed is disclosed by pen registers.” *United States v. New York Tel. Co.*, 434 U.S. 159, 167 (1977) (emphasis added).

Requiring this capability also violates Director Freeh’s assurance to Congress that law enforcement would acquire call-identifying information under CALEA “as it does today – no more, no less,” Joint Hearings at 40, and Congress’s concomitant understanding that it was not expanding the types of information law enforcement could obtain, House Rep. at 17. The DOJ/FBI petition acknowledged that law enforcement has never previously been able “to obtain information that a particular participant was placed on hold during, or dropped from, a multi-party call, because such information resided within, and required access to, the switch.” DOJ/FBI Petition at 44. (J.A. \_\_.) Indeed, the FBI could identify only “the range of participants who might be involved in a multi-party call” and would have to “infer specifically which participants heard portions of the call.” *Id.*

### 3. *Subject-Initiated Dialing and Signaling Information*

This capability requires carriers to send a signal to law enforcement when an intercept subject activates or signals his intent to use a service such as call forwarding, call waiting, or three way calling. Order ¶ 76. The Order states – again without justification or explanation – that signals about call forwarding activation or deactivation identify the direction and destination of a call, and that call waiting signals identify the origin and termination of a call. *Id.* ¶ 82.

Again, however, CALEA requires carriers to give law enforcement only *the specific telephone numbers* associated with a call. If a subscriber switches from one call to another using call-waiting, there are *two* calls in progress, both of which are identified by the J-Standard. Switching back and forth between them does not constitute the “termination” of the first call. The FCC itself has explained that call waiting “enables the subscriber to answer the second call

*without terminating the first call.*” *AT&T Corp. v. Bell Atlantic*, 14 FCC Rcd. 556 ¶ 62 (1998) (emphasis added). Moreover, the FCC’s attempt to equate a call waiting signal with the communication’s “origin” dissolves into incoherence. If a friend calls an intercept subject, the “origin” of that communication is the friend’s phone number (information that is provided by the J-Standard). According to the FCC, if the subject has call waiting, switches to a second call, and then switches back to the friend’s call, that second switch also signals the “origin” of the call with the friend. Thus, under the FCC’s interpretation, the call between the subject and his friend has *two* entirely different “origins” – the friend’s phone number and the flash signal used by the subject to resume the conversation.

An intercept subject’s *activation* of call forwarding service – which occurs before any call has been forwarded – also does not identify the “origin, direction, destination, or termination” of a communication, because no communication has taken place. But the FCC’s Order requires a carrier to report two purportedly “call-identifying” items – the activation of call forwarding and the deactivation – even if no communication is *ever* forwarded. Such signals are not “identifying” any “call” within the meaning of CALEA.

#### 4. *In-Band and Out-of-Band Signaling*

The FCC determined that signals such as ringing, busy, and voice mail waiting constitute call-identifying information because they “indicate information about the termination of a call.” Order ¶¶ 83, 89. And the FCC found that other, unspecified signals may constitute “call identifying information” despite the fact that some of these signals “are not used for call processing.” *Id.*

In-band/out-of-band signals have nothing to do with the numbers dialed and are not otherwise used for routing calls. In most cases, they are not even associated with a “communication” as defined in Title III and incorporated into CALEA. 18 U.S.C. § 2510(1);

47 U.S.C. § 1001(1). Rather, they are associated with call *attempts* that do not result in a communication. A busy signal, for example, does not identify the “termination” of a communication, since no communication has occurred. Moreover, ringing, busy, and similar signals do not provide information about the “termination” of a call because “termination” refers to the final connection necessary to complete the circuit for a communication, not to the temporal end of the call.<sup>7</sup> Thus, as used in the definition of call-identifying information, termination refers only to the telephone number to which a calling party is connected as a result of dialing an initial sequence of digits.

Signals that “are not used for call processing” do not constitute call identifying information. In CALEA, Congress amended ECPA to clarify that law enforcement may use a pen register to record or decode only “dialing and signaling information *utilized in call processing.*” 18 U.S.C. § 3121(c) (emphasis added).

To the extent that the out-of-band signaling required by the FCC includes signaling related to information services, such signaling falls outside of CALEA altogether because information services are exempt from its requirements. *See* 47 U.S.C. § 1002(b)(2)(A). A signal to a telephone indicating that the subscriber has voice mail, for example, is part of an information service (i.e., voice mail), and could not be required under CALEA even if it were call-identifying information. *Id.* § 1001(6)(i)(B) (exempted information services include “a service that permits a customer to retrieve stored information from . . . information storage facilities”).

---

<sup>7</sup> *See, e.g., Telephone Number Portability*, Notice of Proposed Rulemaking, 10 FCC Rcd 12350, 12351 ¶ 1 (1995) (“A telephone number generally identifies the specific telecommunications customer being called, as well as the *termination* point of the call.” (emphasis added)).

**E. The FCC’s Conclusion That the Added Capabilities Are “Reasonably Available” Is Arbitrary and Capricious.**

CALEA requires a carrier to provide “call-identifying information” only if it is “reasonably available” to the carrier. 47 U.S.C. § 1002(a)(2). If it is not, “the carrier does not have to modify its system to make it available.” House Rep. at 22. The FCC acknowledged that, in addition to technical considerations, the cost of a capability is a significant factor in determining whether particular information is “reasonably available.” Order ¶ 29.

When it came to evaluating cost information, however, the FCC made no effort to provide a reasoned basis for its decision and resorted instead to mere *ipse dixit*. Numerous commenters submitted data to the FCC concerning the costs of CALEA. Petitioner USTA estimated, based on data collected from its members, that local exchange carriers alone would have to spend between \$2.2 and \$3.1 billion to implement the J-Standard and six of the capabilities demanded by the FBI. USTA Comments at 8. (J.A. \_\_\_.) GTE stated that its own costs for implementing just the J-Standard would be \$569 million, while SBC said its total costs for compliance with the J-Standard would total approximately \$363 million. Order ¶ 25.

The FCC adopted as a “guide” the estimates submitted by a handful of telecommunications equipment manufacturers that they would earn revenues of \$916 million for sales of CALEA-compliant software designed to meet the J-Standard and \$414 million to implement the additional capabilities demanded by the FBI. *Id.* ¶ 30. In focusing on this data, the FCC did not even discuss record information concerning most *hardware* costs, or the carriers’ costs for testing, engineering, installation, and training in connection with the new capabilities. *See id.* ¶ 25 (noting comments of AirTouch, GTE, and SBC). The only justification the FCC provided for its choice was an unexplained assertion in a footnote that, “relative to other

cost/revenue estimates submitted in this proceeding, we find the manufacturers' estimates to be the most detailed and reliable." *Id.* ¶ 30 n.68.

After asserting that the \$414 million is "not so exorbitant as to require us to reject the punch list automatically," the FCC – without articulating any standard for evaluating cost – said that it would "evaluate" individually the cost of each additional capability. *Id.* ¶ 30. But those "evaluat[ions]" contained nothing more than the identical assertions that costs would be "not so exorbitant" and fell far short of even minimal standards of reasoned decisionmaking:

- Dialed digit extraction: 29 percent of total punch list cost for wireline carriers and 26 percent for wireless carriers, amounting to well over \$100 million under the FCC's estimates, not "so exorbitant as to require automatic exclusion of the capability." Order ¶ 123.
- Hold/join/drop: \$60-plus million "not so exorbitant as to require automatic exclusion of the capability." *Id.* ¶ 75.
- Dialing/signaling information: \$16 million "not so exorbitant as to require automatic exclusion of the capability." *Id.* ¶ 82.
- In-band/out-of-band signaling information: \$50-plus million "not so exorbitant as to require automatic exclusion of the capability." *Id.* ¶ 89.

Whether costs are "not so exorbitant" says nothing about whether the measures are *cost-effective* or *reasonably available* as required by CALEA. 47 U.S.C. §§ 1002(a)(1), 1006(b)(1).<sup>8</sup> "To state a conclusion is not to reason," *Building & Constr. Trades Dep't, AFL-CIO v. Martin*, 961 F.2d 269, 277 (D.C. Cir. 1992), and the FCC's failure to reason requires that its decision be vacated.

---

<sup>8</sup> Furthermore, the word "exorbitant" means "not within the orbit or scope of the law." Webster's Third New International Dictionary 797 (1976). The FCC's statements that its requirements were "not so exorbitant" imply that they were *somewhat* exorbitant, and, therefore, somewhat outside "the orbit or scope of the law."

## **II. THE FCC UNLAWFULLY FAILED TO EVALUATE THE STATUTORY CRITERIA FOR IMPOSING CALEA REQUIREMENTS BY RULEMAKING.**

Even where the FCC found that a capability could be required under the terms of CALEA, the agency had no authority to require that the capability be implemented unless it satisfied five conditions specified in the statute. The FCC may “establish, by rule, technical requirements or standards that”

- meet the assistance capability requirements by cost-effective methods;
- protect the privacy and security of communications not authorized to be intercepted;
- minimize the costs of such compliance on residential ratepayers;
- encourage the provision of new technologies and services; and
- provide reasonable time and conditions for compliance.

47 U.S.C. § 1006(b).

Although the FCC acknowledged the need to analyze and apply these five statutory criteria, Order ¶ 9, it failed to do so anywhere in its Order. The Order, for example, contains no findings that any of the added capabilities are cost-effective. The FCC acknowledged that dialed digit extraction was by far the most expensive of the additional capabilities sought by the FBI, *see id.* ¶ 123, and recognized that law enforcement could obtain the same information by other means, *id.* ¶¶ 120-21. Furthermore, even the government acknowledged that subscribers could foil law enforcement’s objective in obtaining dialed digits from local carriers – identifying the recipient of a calling-card call – by hitting zero and giving the phone number to an operator rather than using the telephone’s keypad. *See Reply Comments of DOJ/FBI at 43 n.26 (June 12, 1998). (J.A. \_\_\_.)* Yet the FCC did not even attempt to compare the costs and expected benefits of this capability with the costs and benefits of the alternatives, and thus had no basis to determine whether this capability is “cost-effective.”

Similarly, section 1006(b)(3) requires the FCC to minimize costs to residential ratepayers. Where, as here, all parties (including the FCC) acknowledge that the combined cost of the J-Standard and the punch list items would far exceed the \$500 million set aside for reimbursing carriers for CALEA compliance, 47 U.S.C. § 1009, the potential effect on ratepayers plainly is significant. Yet the FCC does not even discuss what effect, if any, its Order will have on rates for telecommunications services.

The FCC likewise does not even mention the effects of its Order on incentives to invest in new technologies and services, let alone ensure that the new requirements will “encourage” such investment. *See* 47 U.S.C. § 1006(b)(4). In fact, imposing hundreds of millions of dollars in costs for network modifications that carriers would not otherwise undertake inevitably will divert resources away from the development and deployment of new services. Moreover, the FCC ignored the likely effects of its location ruling on continued demand and innovation in the mobile telephone market. Customers concerned about tracking may turn off their mobile phones or avoid using them altogether. A perception that every wireless telephone can double as a government tracking device would create a significant disincentive to the acceptance and use of wireless technology. Contrary to the express purpose of CALEA, this would harm consumers as well as the wireless industry, and would inevitably slow down the pace of technological innovation.

The FCC’s utter failure to consider these factors and make a reasoned judgment about whether its modifications to the industry standard satisfied these five statutory criteria requires that its Order be vacated. *See, e.g., Nichols v. Board of Trustees*, 835 F.2d 881, 894-95 (D.C. Cir. 1987) (agency decision “cannot stand” where it fails “to discharge its duty to reach an express and considered conclusion with respect to each” statutory factor); *Getty v. Federal Saving and*

*Loan Ins. Corp.*, 805 F.2d 1050, 1055 (D.C. Cir. 1986) (“Stating that a factor was considered . . . is not a substitute for considering it. We must make a ‘searching and careful’ inquiry to determine if [the agency] actually did consider [the statutory factors].”).

### **III. THE FCC REQUIRED DELIVERY OF PACKET-BASED COMMUNICATIONS WITHOUT AN ADEQUATE RECORD AND UNDER CONDITIONS VIOLATING TITLE III AND THE FOURTH AMENDMENT.**

Despite acknowledging that the record did not sufficiently address digital packet communications technologies, the FCC ordered carriers to adapt their systems to provide packet information to law enforcement. That decision was arbitrary and capricious. Moreover, the Order permits carriers to deliver the content of packet-mode communications to a law enforcement agency even when the agency has not satisfied the stringent warrant requirements of Title III and the Fourth Amendment. That result upsets the fundamental balance of the constitutional and statutory principles governing electronic surveillance and therefore violates CALEA.

“Packet-based” networks operate by dividing a communication into small segments and transmitting each segment, or “packet,” separately through the network. A packet consists of a body that contains a portion of the communication’s content and a header that identifies the recipient’s network address and makes it possible to reassemble the stream of packets at the receiving end. Each packet in a single communication may take a different route through the network, depending on network traffic and other conditions. These complex networks are different in kind than traditional switched circuit networks and require special adaptations to support the capabilities preserved by CALEA.

It is not disputed that law enforcement agencies may intercept packet communications under Title III. There was, however, a dispute before the FCC over whether the development of

packet-based technologies have reached a point where it is appropriate to adopt a CALEA standard for them. A number of parties urged the FCC not to adopt *any* capability requirements at this time in order to avoid chilling innovation. *See, e.g.*, AT&T Comments at 25 (Dec. 14, 1998); U S WEST Comments at 27-29 (Dec. 14, 1998). (J.A. \_\_, \_\_.) Parties also disputed whether it was technically and economically feasible to provide packet headers without simultaneously providing packet content. The J-Standard demurred, supporting delivery of packet headers either separated from or together with packet content. J-STD §§ 4.5.2, 5.4.6, 6.3.6. (J.A. \_\_.)

In its Further NPRM, the FCC recognized that the application of CALEA to packet communications raises fundamental questions, including the meaning of call-identifying information in the packet context, the feasibility of separating such call-identifying information from the contents of packets, and the likely impact of a packet-technology rule on cost, privacy, and innovation. *See* Further NPRM ¶¶ 65-66. (J.A. \_\_.) The FCC's Order, however, offered no answers on *any* of these critical issues.

Instead, the FCC concluded that the record did not “sufficiently address” how to apply CALEA to packet technologies. Order ¶ 55. Because it believed that “further efforts can be made to find ways to better protect privacy by providing law enforcement only with the information to which it is lawfully entitled,” the Commission asked the TIA, which functions in part as a standard-setting body, to report by September 2000 regarding how to better address privacy concerns in packet networks. *Id.*

Despite the admittedly inadequate record, the FCC acceded to the FBI's demand to intercept packet communications. The FCC determined that “packet-mode communications, including call-identifying information and call content, may be delivered to law enforcement”

regardless of legal authorization while the agency conducts further proceedings. Order ¶ 55.

The FCC required carriers to comply with this provision by September 2001, only one year after TIA will submit a report addressing the record deficiencies on packets. *Id.* The FCC noted, but ignored, that law enforcement can acquire call-identifying information from a carrier's records, and that its solution raises significant privacy concerns. *Id.* ¶¶ 55 n.107, 56. The agency concluded that privacy would be adequately protected, in the interim, because Title III prohibits law enforcement agencies "from using any content information in a court proceeding if it has only a pen register or trap and trace authorization." *Id.* (citing 18 U.S.C. §§ 2515, 2518).

**A. Applying CALEA to Packet Communications in the Face of a Concededly Deficient Record Was Arbitrary and Capricious.**

The FCC conceded that the record did not "sufficiently address[] packet technologies and the problems that they may present for CALEA purposes," Order ¶ 55, but nonetheless required carriers to deliver packet communications to law enforcement agencies. In so doing, the FCC violated its obligation to "examine the relevant data and articulate a satisfactory explanation for its action including a rational connection between the facts found and the choice made." *Natural Resources Defense Council v. EPA*, 859 F.2d 156, 209 (D.C. Cir. 1988) (*NRDC*) (quotation marks omitted) (quoting *Motor Vehicles Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983)); 5 U.S.C. § 706(2)(A).

The FCC acted on nothing more than an unsubstantiated assumption that packet headers constitute call-identifying information, even though it had recognized in the Further NPRM that this was an unresolved question. And it permitted delivery of content under a pen register order without deciding whether it was feasible to separate headers from content. The FCC should have addressed these issues before imposing any obligations on packet communications. The FCC not only failed to establish a "rational connection between the facts found and the choice made,"

*NRDC*, 859 F.2d at 209, but it arbitrarily imposed this requirement in the conceded absence of any supporting facts.

Further, by adopting these capability requirements on an “interim” basis, the FCC failed to conduct notice and comment required by the Administrative Procedure Act. *See, e.g., Kooritzky v. Reich*, 17 F.3d 1509, 1513 (D.C. Cir. 1994) (agencies must “alert[] interested parties to the possibility of the agency’s adopting a rule different than the one proposed”). The FCC gave no notice that it might order compliance while the standard would be revisited, and likely modified, in the near future.

This “shoot first, aim later” approach creates the risk that the industry will be forced to waste substantial time, effort, and expenditure, or that the agency will simply seek to validate its pre-determined conclusion in future rulemaking. Industry must start working today to achieve compliance with the FCC’s September 2001 implementation deadline, even though beginning with TIA’s report in September 2000, the FCC will be conducting new proceedings that could result in reversing its prior directive. Proceeding in this fashion is irrational.

**B. The FCC Exceeded Its Authority under CALEA by Permitting Law Enforcement Agencies To Intercept Content When Prohibited by Title III and by the United States Constitution.**

By permitting law enforcement agencies to intercept communications content outside the strict parameters of Title III and ECPA, the FCC exceeded its statutory authority and undermined protections for the privacy of communications established by statute and by the Constitution. As a result, compliance with the Order will force carriers to violate their duty under CALEA to “protect the privacy and security of communications . . . not authorized to be intercepted.” 47 U.S.C. § 1002(a)(4).

The FCC recognized that its Order permits law enforcement officials to intercept the *contents* of packet communications with nothing more than a pen register authorization. Order

¶ 56. As a result, law enforcement officials would obtain communications content without having to satisfy the stringent procedural and substantive safeguards mandated by Title III, 18 U.S.C. §§ 2516, 2518, and by the Fourth Amendment, *Katz v. United States*, 389 U.S. 347, 353 (1967).

The FCC's only attempt to justify this result is to assert that Title III prohibits law enforcement's *use* of any content evidence obtained in violation of Title III. Order ¶ 56 & n.109. That argument proves far too much – it would justify *always* providing law enforcement officials the entire content of a communication and trusting them to avert their attention from any portions that they are unauthorized to intercept. Title III prohibits the *receipt* of information from unlawful electronic surveillance, not just its use. Similarly, the text of the Fourth Amendment prohibits “unreasonable searches and seizures” themselves; the prohibition on the use of the results of an unreasonable search and seizure is a prophylactic measure designed to remove any incentives to engage in the unlawful search and seizure in the first place. *United States v. Verdugo-Urquidez*, 494 U.S. 259, 264 (1990) (“[A] violation of the [Fourth] Amendment is fully accomplished at the time of an unreasonable governmental intrusion.”). Thus, the FCC turned the law on its head when it found that an admittedly unlawful search or seizure was permissible because law enforcement could not use the fruits of that intrusion.

This conclusion is confirmed by the real-world application of Title III and ECPA. Applying ECPA, the Fourth Circuit has held that pen register authorization does not permit the use of a device that captures traditional dialing information along with certain incidental contents of communications. *Brown v. Waddell*, 50 F.3d 285, 292 (4th Cir. 1995). Tracking the Supreme Court's ruling in *Smith v. Maryland*, the court explained that the fundamental reason for excluding pen registers from the scope of the Fourth Amendment is that such devices' “*only*

*capability* is to intercept” the telephone numbers a person calls. *Id.* at 292 (citing *Smith*, 442 U.S. at 745) (emphasis added).

The FCC’s expansion of law enforcement’s ability to obtain content information contravenes not only the Fourth Amendment and Title III, but CALEA itself. As shown above, CALEA contains no authorization for law enforcement to engage in electronic surveillance; rather, it ensures that law enforcement can carry out surveillance that is authorized by other laws. *See supra* at 5-6. CALEA was intended only to “preserve a narrowly focused capability” to carry out “*properly authorized* intercepts.” House Rep. at 13 (emphasis added). Even the FBI expressly disavowed any intention to expand existing surveillance law. Joint Hearings at 6-7. Thus, CALEA did not grant the FCC any power to expand law enforcement’s authority to conduct electronic surveillance, and its decision to require carriers to deliver content information to law enforcement officials who lack the requisite Title III authorization was *ultra vires*.

**CONCLUSION**

For the foregoing reasons, the Court should vacate all challenged portions of the FCC's Order and remand the matter to the FCC for any necessary further proceedings consistent with its opinion.

Respectfully submitted,

---

Theodore B. Olson  
Eugene Scalia  
Montgomery N. Kosma  
GIBSON, DUNN & CRUTCHER LLP  
1050 Connecticut Avenue NW  
Washington, D.C. 20036-5303  
(202) 955-8500

Michael Altschul  
Cellular Telecommunications Industry Association  
1250 Connecticut Avenue NW, Suite 800  
Washington, D.C. 20036  
(202) 785-0081

Jerry Berman  
James X. Dempsey  
Center for Democracy and Technology  
1634 Eye Street NW, Suite 1100  
Washington, D.C. 20006  
(202) 637-9800

*Counsel for Cellular Telecommunications  
Industry Association and Center for Democracy  
and Technology*

January 20, 2000

---

John H. Harwood II  
Lynn R. Charytan  
Samir Jain  
WILMER, CUTLER & PICKERING  
2445 M Street NW  
Washington, D.C. 20037  
(202) 663-6000

Lawrence E. Sarjeant  
Linda L. Kent  
Keith Townsend  
John W. Hunter  
Julie E. Rones  
United States Telecom Association  
1401 H Street, Suite 600  
Washington, D.C. 20036  
(202) 326-7248

*Counsel for United States Telecom  
Association*

## **CERTIFICATE OF COMPLIANCE**

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify that this brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B). The brief uses a 12-point proportionately-spaced font, and, based on the count supplied by the word processor used to prepare the brief, it contains 11,137 words.

---

Samir Jain

**CERTIFICATE OF SERVICE**

I DO HEREBY CERTIFY that on this 20<sup>th</sup> day of January, 2000, I caused two true and correct copies of the foregoing Brief of Petitioners United States Telecom Association, Cellular Telecommunications Industry Association, and Center for Democracy and Technology to be served upon the following parties by Federal Express and hand delivery via messenger:

John E. Ingle  
Federal Communications Commission  
445 Twelfth Street, SW  
Room 8-B201  
Washington, DC 20554

Douglas N. Letter  
Civil Division  
U. S. Department of Justice  
601 D Street, NW  
Room 9106  
Washington, DC 20530

Stewart A. Baker  
Thomas M. Barba  
Matthew L. Stennes  
Steptoe & Johnson, LLP  
1330 Connecticut Avenue, NW  
Washington, DC 20036  
*Counsel for Intervenor  
Telecommunications Industry Association*  
Robert Allen Long, Jr.  
Covington & Burling  
1201 Pennsylvania Avenue, NW  
Washington, DC 20044  
*Counsel for Intervenor  
Sprint Spectrum, L.P.*

Mary McDermott  
Brent H. Weingardt  
Todd B. Lantor  
Personal Communications Industry Association  
500 Montgomery Street, Suite 700  
Alexandria, VA 22314

David A. Gross  
AirTouch Communications, Inc.  
1818 N Street, NW  
Suite 800  
Washington, DC 20036

Sylvia Lesse  
John Kuykendall  
Kraskin, Lesse & Cosson  
2120 L Street, NW  
Suite 520  
Washington, DC 20037  
*Counsel for Intervenor  
The Rural Cellular Association*

Kurt A. Wimmer  
Gerard J. Waldron  
Covington & Burling  
1201 Pennsylvania Avenue, NW  
Washington, DC 20044  
*Counsel for Petitioners  
EPIC, ACLU and EFF*

Robert B. McKenna  
Kathryn Marie Krause  
U S WEST, Inc.  
1020 19<sup>th</sup> Street, NW  
Suite 700  
Washington, DC 20036

---

Samir Jain

**ADDENDUM A – TABLE OF CONTENTS**

Communications Assistance for Law Enforcement Act, 47 U.S.C. § 1001 *et seq.*,

47 U.S.C. § 1001 .....	1
47 U.S.C. § 1002 .....	3
47 U.S.C. § 1006 .....	6
47 U.S.C. § 1007 .....	9
47 U.S.C. § 1008 .....	11
47 U.S.C. § 1009 .....	14

Title III, Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. § 2510 *et seq.*,

18 U.S.C. § 2510 .....	15
18 U.S.C. § 2515 .....	19
18 U.S.C. § 2516 .....	20
18 U.S.C. § 2518 .....	24
18 U.S.C. § 2522 .....	31

Electronic Communications Privacy Act of 1986, 18 U.S.C. § 3121 *et seq.*,

18 U.S.C. § 3121 .....	33
18 U.S.C. § 3122 .....	34
18 U.S.C. § 3123 .....	35
18 U.S.C. § 3127 .....	37

**ADDENDUM B – TABLE OF CONTENTS**

Third Report and Order, *In the Matter of Communications Assistance  
for Law Enforcement Act*, 14 FCC Rcd 16794 (1999) .....1