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,
ELECTRONIC PRIVACY INFORMATION CENTER,
AMERICAN CIVIL LIBERTIES UNION,
ELECTRONIC FRONTIER FOUNDATION,
CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION,
AND CENTER FOR DEMOCRACY AND TECHNOLOGY,

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

Carlos Perez-Albuerne
Mark D. Cahill
Lawrence A. Friedman
Kathleen A. Burdette
CHOATE, HALL & STEWART
Exchange Place
53 State Street
Boston, Massachusetts 02109-2891
(617) 248-5000
Counsel for Petitioners

Kurt A. Wimmer
Gerard J. Waldron
Russell D. Jessee*
Margaret H. Grebe*
COVINGTON & BURLING
1201 Pennsylvania Ave., N.W.
Washington, D.C. 20037
(202) 662-6000
Counsel for Petitioners

(Additional counsel listed on inside cover)

January 20, 2000

David L. Sobel, Esq.
Marc Rotenberg, Esq.
ELECTRONIC PRIVACY INFORMATION CENTER
666 Pennsylvania Avenue, S.E., Suite 301
Washington, D.C. 20003
Counsel for the Electronic Privacy Information Center

Shari Steele, Esq.
ELECTRONIC FRONTIER FOUNDATION
1550 Bryant Street, Suite 725
San Francisco, California 94103
Counsel for the Electronic Frontier Foundation

Barry Steinhardt, Esq.
AMERICAN CIVIL LIBERTIES UNION
125 Broad Street
New York, New York 10004
Counsel for the American Civil Liberties Union

* Members of the bars of Virginia and Wisconsin,
respectively; not yet admitted in the District of Columbia.

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

Pursuant to Circuit Rule 28(a)(1), petitioners Electronic Privacy Information Center ("EPIC"), Electronic Frontier Foundation ("EFF") and the American Civil Liberties Union ("ACLU") (collectively, the "Public Interest Petitioners") submit the following information:

(A) **Parties and Intervenors**

Petitioner EPIC is a non-profit, public interest research center whose mission is to focus public attention on emerging civil liberties issues in the field of electronic information. EPIC is sponsored by the Fund for Constitutional Government, a non-profit organization established in 1974 to protect privacy, the First Amendment, and other constitutional rights.

Petitioner EFF is a non-profit, non-partisan organization founded in 1990 that works in the public interest to protect fundamental civil liberties, including privacy and freedom of expression, in the arena of computers and the Internet. It supports litigation and public policy advocacy to preserve, protect and extend constitutional rights within the realm of computing and telecommunications technology.

Petitioner ACLU is a nationwide, non-partisan organization of some 300,000 members dedicated to defending the principles of liberty and equality embodied in the Bill of Rights. Throughout its 75-year history, the ACLU has been particularly concerned with abridgements of the freedoms guaranteed by the Constitution, including bedrock principles ensuring Americans' right to privacy in the digital era.

Other Petitioners. The United States Telecom Association, the Cellular Telecommunications Industry Association and the Center for Democracy and Technology (collectively, the "Telecommunications Petitioners") also are petitioners in this action.

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

Intervenors. 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. have intervened in this action.

(B) **Ruling under Review**

The ruling of which review is sought is the Third Report and Order adopted by the Federal Communications Commission, *In the Matter of Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, FCC 99-230 (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.

(C) **Related Cases**

This case has not previously been before this Court or any other court. The Public Interest Petitioners are not aware of any related cases pending in this Court or any other court.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES AND AGENCY DECISIONS

CONSTITUTIONS AND STATUTES

OTHER MATERIALS

* Authorities upon which we chiefly rely are marked with asterisks.

GLOSSARY

ACLU:	American Civil Liberties Union
CALEA:	Communications Assistance for Law Enforcement Act
Carriers:	Telecommunications Carriers
CDT:	Center for Democracy and Technology
Commission:	The Federal Communications Commission
CTIA:	Cellular Telecommunications Industry Association
DOJ:	Department of Justice
EFF:	Electronic Frontier Foundation
ECPA:	Electronic Communications Privacy Act
EPIC:	Electronic Privacy Information Center
FBI:	Federal Bureau of Investigation
FCC:	Federal Communications Commission
House Report:	H.R. Rep. No. 103-827, pt. 1 (1994)
Order:	*Third Report and Order, Communications Assistance for Law Enforcement Act,* CC Docket No. 97-213, FCC 99-230 (Aug. 31, 1999)
Pen Register Order:	A pen register or trap-and-trace order under 18 U.S.C. § 3122(b)
Title III:	Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. § 2510 *et seq.*
USTA:	United States Telecom Association

JURISDICTIONAL STATEMENT

These consolidated petitions seek review of a final order of the Federal Communications Commission, Third Report and Order, *In the Matter of Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, FCC 99-230 (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.

Petitioners EPIC and ACLU timely filed their joint petition for review in this Court on November 18, 1999. Petitioner EFF timely filed its petition for review in the United States Court of Appeals for the Ninth Circuit on November 18, 1999, and that petition was ordered to be transferred to this Court on December 7, 1999. This Court 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.

RELEVANT STATUTORY PROVISIONS AND REGULATIONS

Pertinent statutory provisions and regulations are set forth in an addendum bound with the brief of the Telecommunications Petitioners.

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,
ELECTRONIC PRIVACY INFORMATION CENTER,
AMERICAN CIVIL LIBERTIES UNION,
ELECTRONIC FRONTIER FOUNDATION,
CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION,
AND CENTER FOR DEMOCRACY AND TECHNOLOGY,

Petitioners,

v.

FEDERAL COMMUNICATIONS COMMISSION
and UNITED STATES OF AMERICA,

Respondents.

**BRIEF OF PETITIONERS
ELECTRONIC PRIVACY INFORMATION CENTER,
ELECTRONIC FRONTIER FOUNDATION, AND
THE AMERICAN CIVIL LIBERTIES UNION**

STATEMENT OF ISSUES PRESENTED FOR REVIEW

1. Whether the Commission's decision to adopt an "interim standard" under which carriers must provide law enforcement authorities with the contents of packet-mode communications under a pen register order was beyond the Commission's statutory authority under CALEA, was arbitrary and capricious in light of the Commission's admitted failure to compile a record on packet-mode communications, and violated Title III.

2. Whether the Commission's decision to require carriers to provide law enforcement with digits dialed by subscribers after the primary call has been placed under a pen

register order was beyond the Commission's authority under CALEA, was arbitrary and capricious, and violated Title III.

3. Whether the Commission's acted arbitrarily and beyond the scope of CALEA in determining that information disclosing the physical location of a caller using a mobile telephone constitutes call-identifying information that must be provided by carriers to law enforcement.

4. Whether the Commission's actions requiring carriers to provide the content of packet-mode communications and post-cut-through digits to law enforcement under pen register orders violates the Fourth Amendment.

STATEMENT OF THE CASE / STATEMENT OF FACTS

The joint statements of the case and facts of all petitioners is contained in the brief of Telecommunications Petitioners.

SUMMARY OF ARGUMENT

This case concerns the fundamental right to privacy held by the American public in the telecommunications and Internet age. Our nation's reliance upon the telecommunications network has never been greater. Yet, the Commission's interpretation of CALEA – a statute intended simply to replicate law enforcement's existing wiretapping capabilities in the digital age[1] – has endangered the public's right to privacy by permitting law enforcement to obtain the actual content of conversations and Internet transmissions without complying with Title III or the Fourth Amendment. For this reason, the *Order* should be vacated.

---

[1] CALEA is meant "to provide law enforcement no more and no less access to information than it had in the past." Testimony of FBI Director Louis Freeh, H.R. Rep. No. 103-827, pt. 1 ("House Report") at 22 (1994).

This case is not, however, an attempt to limit legitimate enforcement of law. The proper resolution of this case will not deny law enforcement access to any information to which it is entitled. The issue here is one of process – whether law enforcement is required to comply with longstanding Title III and Fourth Amendment requirements before gaining access to the content of conversations, content in which individuals hold an expectation of privacy. CALEA does not amend these standards; rather, it demands fidelity to them. Petitioners seek only the enforcement of CALEA's demand that law enforcement be required to follow procedures that guard the public's right to privacy.

The Commission has far exceeded the narrow statutory authority granted it by Congress, and has specifically failed to protect the privacy interests of the public, as demanded by CALEA. *See* 47 U.S.C. § 1006(b)(2). Its *Order* is entitled to no deference from this Court, *see Panamsat Corp. v. FCC*, No. 98-1408, 1999 WL 1215311 at *6 (D.C. Cir. Dec. 21, 1999), which should construe CALEA's requirements *de novo*. *See Professional Airways Sys. Specialists v. Federal Labor Relations Auth.*, 809 F.2d 855, 857 (D.C. Cir. 1987). This analysis will require the *Order* to be vacated.

ARGUMENT

I. THE ORDER EXCEEDS THE COMMISSION'S STATUTORY AUTHORITY UNDER CALEA, FAILS TO COMPLY WITH TITLE III, AND IS ARBITRARY AND CAPRICIOUS.

A. THE ORDER'S "INTERIM STANDARD" FOR PACKET-MODE TRANSMISSIONS IS IRRATIONAL, BEYOND THE COMMISSION'S STATUTORY AUTHORITY AND ENDANGERS PRIVACY INTERESTS IN THE INTERNET AGE.

1. The Vagueness of the Order May Open the Door to the Tapping of the Internet Without Congressional Authorization or Title III and Fourth Amendment Protections.

Packet-mode communication is the transmission technology of the Internet. It is, moreover, becoming increasingly important for the transmission of voice conversations as well as data in today's next-generation telecommunications systems. The pace of digital convergence is accelerating, and packet-mode networks are fast becoming a more dominant feature of our telecommunications landscape.

In traditional telecommunications, a telephone switch establishes a "circuit" between the caller and recipient, and that channel remains open during a call to carry information back and forth. By contrast, in "packet-mode" communication, information – voice or data – is broken down into small pieces of digital electronic information called "packets." Each packet is like an envelope, containing both message content and a header that indicates the point from which the packet originates and the point to which it is being sent. The header of a packet is analogous to a dialed number on a traditional telephone system; the message content is identical to the content of a telephone conversation. Each packet, containing a portion of the message, is transmitted individually. When all the packets reach their destination, they are reassembled into the complete message.

The *Order* recognizes the unique privacy concerns associated with packet technologies – *each packet contains both a header and message content*.[2] The header is call-identifying information that can be obtained (if it could be obtained in isolation) with a pen register order. The message is call content, which cannot be obtained without a Title III warrant. If law enforcement obtains access to an entire packet via a pen register order, then, it would automatically receive call content without a warrant. The Commission recognized that the weight of the record demonstrated that it is currently not feasible to provide access only to the routing information contained in a packet's header separate from the call content in the packet.[3] In light of this technical issue, the Commission correctly saw the need for a specially tailored solution in order to protect privacy interests and guarantee the separation of call content from call-identifying information. Accordingly, it ordered that the record in regard to packet-mode systems be developed further.[4]

But after taking this proper step, the Commission went off track. Incredibly, despite the Commission's recognition that the delivery of the content of messages carried by data packets on a pen register order would violate the Fourth Amendment, the *Order* established an "interim standard" that will require just such a constitutional and Title III violation. Under the "interim standard," carriers will be required to deliver *both* call-identifying and call content information from packets to law enforcement officials under a mere pen register order.

---

[2] *Third Report and Order, Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, FCC 99-230 (Aug. 31, 1999) (the "*Order*"), ¶ 55.

[3] *See id.*, ¶¶ 53-54.

[4] *See id*. ("We believe 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.").

This conclusion is far beyond the scope of CALEA. Congress clearly defined "call-identifying information" to exclude call content. *See* 47 U.S.C. § 1001(2). Congress, moreover, explicitly determined that CALEA should not be read to authorize tapping the Internet under the guise of mere pen register orders.[5] To the extent that the Commission's "interim standard" authorizing law enforcement to receive the *contents* of packets with a pen register order is read to encompass Internet communications, law enforcement could obtain Internet transmissions without a warrant simply by directing a pen-register order to the telephone company carrying the packets rather than by seeking a full warrant against the Internet service provider that receives those packets.[6] This result would vitiate Congress' clear effort to ensure that CALEA would not apply to the Internet.

The same defect is true, of course, of voice and other communications transmitted by packet-mode telecommunications systems. Under the Commission's decision, law enforcement will be permitted to obtain the *substantive content* of messages transmitted by packet-mode

---

[5] *See* 47 U.S.C. §§ 1001(6), 1001(8)(C) ("information services" such as Internet access are not covered by CALEA). As the House Report explained:

> Also excluded from [the] coverage [of CALEA] are all information services, such as Internet service providers or services such as Prodigy and America-On-Line. . . . [T]he definition of "telecommunications carrier" does not include persons or entities to the extent they are engaged in providing information services, such as electronic mail providers, on-line services providers such as Compuserve, Prodigy, America-On-Line or Mead Data, or Internet service providers.

House Report at 18, 20.

[6] The views of law enforcement expressed before the Commission raise this potential:

> [The] statutory distinction between telecommunications carriers and providers of information services does not correspond to any distinction between packet-mode and circuit-mode communications; therefore, the use of packet-mode protocols does not turn the transmission of a wire or electronic communication by a telecommunications carrier into the provision of information services.

Order, ¶ 54 (summarizing FBI argument).

communications, whether that substance is voice or data. This decision is arbitrary and capricious and far beyond the scope of CALEA.

2. The Commission's "Interim Standard" Should Be Vacated Because It Is Arbitrary and Capricious, Rests on an Admittedly Incomplete Record, and Permits Orders that Violate Title III.

The Commission recognized that the record it had compiled was insufficient to support any decision regarding the unique problems of packet technologies and ordered further review by industry groups to craft a permanent standard that protects privacy.[7] Inexplicably, however, the Commission did not await the findings of this new inquiry before acting. Rather, it created an "interim standard" under which law enforcement will be granted access to the entirety of packets for the purpose of obtaining call-identifying information – without requiring that telecommunications carriers exclude call content.

Requiring carriers to provide law enforcement with the call content that is carried in packets is contrary to CALEA, Title III and well-settled law. To obtain call content information under a wiretap order, law enforcement is required to satisfy a much more demanding standard than is required to obtain call-identifying information under a pen register device. The public has a reasonable expectation of the privacy of its conversations, an expectation that courts have held does not extend to telephone numbers called.[8] To obtain a wiretap warrant to seize call content, law enforcement must show, *inter alia*, that the information sought is in connection with a specific crime; that probable cause exists that the crime is being committed or about to be committed by a particular individual; and that communications concerning the crime will be

---

[7] *Id.*

[8] *See Smith v. Maryland*, 442 U.S. 735, 745 (1979).

obtained through use of the wiretap.[9] A law enforcement agency may obtain a pen register device order merely by demonstrating that the information "likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency."[10]

Although CALEA authorizes the Commission to promulgate regulations concerning law enforcement's ability to intercept communications and call-identifying information, the statute explicitly allows such interception and access "only in accordance with a court order or other lawful authorization." 47 U.S.C. § 1004; *see also* 47 U.S.C. § 1002(a)(1). Title III provides the statutory scheme to authorize law enforcement's interception of communications, *see* 47 U.S.C. §§ 2516, 2518, and CALEA requires the Commission to promulgate standards that reflect Title III's limitations placed upon law enforcement's access. These limitations include requiring law enforcement to make a detailed showing of particularized suspicion, efficacy, and need for electronic interception of communication content before surveillance can commence.[11] This is a much more demanding standard than law enforcement must meet to obtain call-identifying information via a pen register order.

The Commission correctly noted that allowing law enforcement with a pen register order to obtain the call content of packets violates the mandate in CALEA §103(a)(4)(B) that telecommunications carriers provide information to law enforcement "in a manner that protects . . . the privacy and security of communications . . . not authorized to be intercepted."[12] The Commission itself suggested the proper interim solution. In its *Order*, the Commission finds that

---

[9] 18 U.S.C. § 2521(c)(3).

[10] 18 U.S.C. § 3122(b).

[11] *See* 18 U.S.C. § 2518(1)(b).

[12] Further Notice of Proposed Rulemaking, *In re Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, FCC 98-282 (rel. Nov. 5, 1998), ¶ 63.

any call-identifying information sought by law enforcement may also be acquired, *separate from content*, from a carrier's transmission records.[13] This readily available alternative is the best means of both preserving the status quo by protecting privacy interests and aiding law enforcement. The Commission opted not to pursue this administratively and constitutionally sound alternative, claiming that its interim solution – allowing unauthorized access to call content –is supported by CALEA itself.

This decision, and the interim standard that resulted from it, was not supported by the statute. 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, of equal importance, is intended to uphold the privacy interests of the American public.[14] Congress emphasized that the statute's requirements would serve as "both a floor and a ceiling" on government surveillance demands[15] and thus limit the surveillance capabilities of law enforcement.[16] Congress recognized that "as the potential intrusiveness of technology increases, it is necessary to ensure that government surveillance

---

[13] *Order*, n.107.

[14] 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).

[15] House Report at 22.

[16] *See* House Report at 18 ("It is also important from a privacy standpoint to recognize that the scope of the legislation has been greatly narrowed"); *id*. at 22-23 ("The Committee urges against overbroad interpretation of the requirements. . . . The committee expects industry, law enforcement and the FCC to narrowly interpret the requirements").

authority is clearly defined and appropriately limited."[17] Congress directed the telecommunications industry, law enforcement and the Commission "to narrowly interpret" the requirements of CALEA.[18]

The Commission asserts that the law enforcement agency itself will protect the privacy interests threatened by the interim standard.[19] This decision explicitly violates Section 103(a)(4) of CALEA, which requires the *carriers* to protect communications not authorized to be intercepted. It is also based on an unrealistic assumption that law enforcement will impose severe self-restraint in processing the information, a proposition with which most Americans undoubtedly would disagree.[20]

In sum, the Commission's interim packet-mode standard is fatally flawed and erodes the congressional privacy protection built into CALEA because it requires telecommunications carriers to provide call-identifying information *and* call content information in cases where law enforcement is authorized to receive only the former. If the distinction between call-identifying information and call-content information is eroded for packet-mode communications, the privacy protections implemented by Congress and courts and relied on by the public will all but disappear. This outcome would be ominous because packet-mode communication is swiftly becoming the telecommunications technology of choice for today's Internet age.

---

[17] *Id.* at 17.

[18] *Id.* at 23.

[19] *Order*, ¶ 56.

[20] As Judge Posner has noted, "in the absence of market discipline, there is no presumption that the government will strike an appropriate balance between disclosure and confidentiality." Posner, *The Uncertain Protection of Privacy by the Supreme Court*, 1979 Sup. Ct. Rev. 173, 176.

B. THE COMMISSION ERRED IN PERMITTING LAW ENFORCEMENT TO OBTAIN POST-CUT-THROUGH CONTENT WITH ONLY A PEN REGISTER ORDER.

Callers using current telephone technology such as voice mail often enter additional touch-tone digits after having "dialed" to make the connection to the original called party. The *Order* requires carriers to provide to a law enforcement agency with only a pen register order not only the original call-identifying digits but also all non-call-identifying digits subsequently entered.[21] This requirement is unlawful because it violates CALEA's instructions and violates Title III. The Commission improperly sacrificed privacy to expand law enforcement authority by requiring easy access to so-called "post-cut-through dialed digits" without regard to whether the digits are part of a call's contents.

1. Some Post-Cut-Through Dialed Digits Constitute Call Content, Which Is Available To Law Enforcement Only With A Title III Warrant.

An originating carrier uses the first set of numbers that a caller dials to identify the called party and complete the call. Numbers that a caller dials after the originating carrier has completed a circuit are called post-cut-through dialed digits. These post-cut-through digits often convey substantive information, such as credit card numbers, bank account numbers, voicemail passwords, responses to automated systems. Rather than identifying any call routing information needed to complete the call, these digits are analogous to spoken words – indeed, many banks permit account holders to check balances either by speaking to a teller or pressing keys on a telephone. Clearly, post-cut-through dialed digits can constitute the "contents" of a call, which Congress defined to include "any information concerning the substance, purport, or meaning of

[21] O*rder*, ¶ 123.

that communication."[22] Accordingly, access to this post-cut-through information – whether it is digits or words – should require a Title III warrant.[23]

In other cases, a caller using a prepaid calling card dials a toll-free number to reach the card's long-distance carrier and then, after the cut-through to the long-distance carrier, dials post-cut-through digits to reach the ultimate called party. Comments from the telecommunications industry universally establish that, from the originating carrier's standpoint, such digits are outside the purview of the initiating carrier once a subscriber has connected to a long-distance carrier. Nonetheless, the Commission concluded that *some* digits dialed after connecting to a long-distance carrier identify the "origin, direction, destination or termination" of the communications and thus are call-identifying information under CALEA.[24] Consequently, the Commission required that originating carriers provide access to *all* post-cut-through dialed digits once law enforcement has obtained a mere pen register order.[25]

The Commission adopted this standard after rejecting three alternatives to its own over-inclusive proposal.[26] The Commission incorrectly observed that "there appears to be a consensus" that law enforcement should be permitted access to digits dialed by the subject after connecting to another carrier's service simply because one trade association and two Bell companies proposed less-costly alternatives to a Commission proposal that would impose

---

[22] 18 U.S.C. § 2510(8); *see* 47 U.S.C. § 1001(1) (adopting definitions of 18 U.S.C. § 2510).

[23] *See* 18 U.S.C. §§ 2516, 2518 (providing statutory scheme for law enforcement to obtain warrants to intercept communications).

[24] *Order*, ¶ 119.

[25] *Id.*, ¶ 123.

[26] *See id.*, ¶¶ 120-122.

significant costs on originating carriers.[27] There is no basis in the record, however, much less a consensus, for the conclusion that law enforcement should be able to obtain *all* post-cut-through dialed digits from the originating carrier.[28] Moreover, the record provides no basis for concluding that law enforcement should be able to obtain *all* post-cut-through dialed digits merely with a pen register order. The Telecommunications Industry Association (which represents all major equipment manufacturers), the Public Interest Petitioners, and other commenters showed that some post-cut-through dialed digits constitute call content that must not be revealed to law enforcement through a pen register order served on the local carrier.[29]

2. The Commission Ignored CALEA's Mandate To Protect Privacy and Ignored Title III.

For the Commission to require a capability in addition to the J-standard, it must "protect the privacy and security of communications not authorized to be intercepted."[30] In its *Order*, the Commission paid lip-service to concerns about "privacy implications," but it nonetheless required access to call contents with only a pen register order.[31] Clearly, some post-cut-through dialed digits are part of a call's contents, while others may be viewed as call-identifying information. It is equally clear that with current dialed digit extraction technology, law enforcement will obtain call-content post-cut-through digits intermixed with call-identifying post-cut-through digits. The *Order* does not protect privacy interests at all. Rather, it wholly abrogates the privacy protection for call contents afforded by Title III's warrant standards. The

---

[27] *See id.*, ¶ 120.

[28] *See, e.g.*, BellSouth Comments at 18-19; PCIA Comments at 33-34; SBC Comments at 18.

[29] *See, e.g.*, TIA Comments at 42-43; EPIC/EFF/ACLU Comments at 27.

[30] 47 U.S.C. § 1008(b)(2).

[31] *Order*, ¶ 123.

Commission stated that "[w]e do not believe that CALEA contemplates changing the standard of proof in obtaining a warrant in order to avoid implementing a particular CALEA feature."[32] Clearly, the Commission is correct in this belief. Yet, the Commission, acting far outside its area of competence (and thus deprived of any *Chevron* deference), changed the standard of proof necessary to access dialed digits that constitute content to implement a particular CALEA feature. 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's contents, law enforcement has no authority to obtain access to those digits on a pen register order.[33]

The *Order*'s solution is not, however, the only route for law enforcement. Law enforcement agencies have two avenues to obtain call-identifying post-cut-through digits while protecting the public's privacy: (1) serving the originating carrier with a Title III warrant to obtain all dialed digits, both content and call-identifying information, or (2) having the originating carrier identify the long-distance carrier in question and then serving that carrier with a pen register order to obtain the call-identifying digits. Requiring the heightened protection of a Title III warrant for all post-cut-through digits, while potentially cumbersome for law enforcement, certainly is more consistent with CALEA's mandate to consider privacy interests than is the Commission's current solution that capriciously ignores those interests. Likewise, requiring law enforcement agencies to take the added steps of identifying the second entity and

---

[32] *Id.*, ¶ 120.

[33] *See Brown v. Waddell*, 50 F.3d 285, 294 (4th Cir. 1995) (holding that duplicate digital display pager used to intercept numeric transmissions is not "pen register" under ECPA and its use by law enforcement without was "unauthorized interception of 'electronic communications'" as matter of law).

serving it with a pen register order, while more cumbersome, protects privacy consistent with CALEA's mandate.[34]

Furthermore, the Commission arbitrarily rejected the option of serving the second entity with a pen register order by finding that the method could be time-consuming and that it "would seem to defeat one of the purposes of CALEA to preserve the ability of law enforcement officials to conduct electronic surveillance effectively and efficiently in the face of rapid advances in telecommunications technology."[35] The Commission simply invented the "effectively and efficiently" goal; CALEA does not contain any mandate to ensure that law enforcement can conduct surveillance "effectively and efficiently." Rather, Congress enacted CALEA 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."[36] The *Order* therefore is beyond the scope of CALEA and should not stand.

If nothing else, the *Order* must be vacated because it violates Title III. The *Order* permits law enforcement "to access non-call-identifying digits (such as bank account numbers) with only a pen register warrant." *Order*, ¶ 123. To the extent that the *Order* gives law enforcement access to call contents without obtaining a warrant based on, *inter alia*, a proper showing of particularized need and probable cause, *see* 18 U.S.C. § 2518(1), (3), the *Order* is unlawful.

---

[34] "[CALEA] is not intended to guarantee 'one stop shopping' for law enforcement." House Rpeort at 22.

[35] *Order*, ¶ 121.

[36] House Report at 13.

C. THE COMMISSION ERRED IN ADOPTING LOCATION TRACKING PROVISIONS THAT ARE UNAUTHORIZED BY CALEA.

The Commission wrongly determined that CALEA requires wireless carriers to provide law enforcement with information on their subscribers' location at the beginning and end of each call. CALEA does not contemplate the conversion of mobile telephones into location-monitoring devices; this information was never available in the analog environment, and there is no reasoned justification for including it in CALEA. The plain language of CALEA provides that "call identifying information shall not include any information that may disclose the physical location of the subscriber." 47 U.S.C. § 1002(a)(2)(B). Given the clarity of the statute, the Public Interest Petitioners opposed this requirement when the telecommunications industry agreed to its inclusion in the J-Standard, and again opposed it before the Commission. As then-FBI Director Freeh testified:

> [Call setup information] does not include any information which might disclose the general location of a mobile facility or service, beyond that associated with the area code or exchange of the facility or service. There is no intent whatsoever, with reference to this term, to acquire anything that could properly be called "tracking" information.[37]

This view is undoubtedly correct, and the Commission plainly acted beyond the terms of CALEA in requiring carriers to provide law enforcement with information it never sought before Congress.

We support the legal arguments of the Telecommunications Petitioners on this point and urge the Court to vacate the *Order*'s incorrect conclusion that CALEA requires the provision of any location monitoring information to law enforcement.

---

[37] Joint Hearings on H.R. 4922 and S. 2375, 103d Cong. 29 (1994).

II. THE ORDER MUST BE VACATED BECAUSE IT MANDATES UNCONSTITUTIONAL SEARCHES AND SEIZURES.

As discussed above, the *Order* requires telecommunication carriers to supply both packet-mode communications and post-cut-through dialed digits to law enforcement officers who have obtained a pen register order. Both packet-mode communications and post-cut-through digits convey call content intermixed with call identifying information and are, therefore, subject to the warrant requirements imposed by the Fourth Amendment in addition to those imposed by Title III. By ordering carriers to provide law enforcement with access to electronic communication *content* without first having law enforcement obtain the constitutionally required warrant, the *Order* compels carriers to engage in illegal searches and seizures. Because the Commission lacks the authority to modify the requirements of the Fourth Amendment, the *Order* must be vacated.

A. THE *ORDER* IMPLICATES PRIVACY INTERESTS PROTECTED BY THE FOURTH AMENDMENT.

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const., amend. IV. A search or seizure, within the meaning of the Fourth Amendment, occurs when the government infringes an individual's legitimate expectation of privacy. *See Katz v. United States*, 389 U.S. 347, 353 (1967). Whether an individual has a legitimate expectation of privacy depends upon (1) whether the individual has exhibited a subjective expectation of privacy, and (2) whether that subjective expectation is "one that society is prepared to recognize as 'reasonable.'" *See Smith v. Maryland*, 442 U.S. 735, 740 (1979) (quotation omitted).

Courts have consistently held that an individual has a reasonable and legitimate expectation of privacy in the content of telephone communications. *See Smith*, 442 U.S. at 741; *Katz*, 389 U.S. at 353. Those reasonable expectations persist when the individual uses cellular

telecommunications or other new technologies. In *Smith v. Maryland*, the Court articulated the constitutional distinction between call content and call identifying information for purposes of Fourth Amendment analysis. *See Smith*, 442 U.S. at 741. The Court concluded that surveillance via a pen register device does not implicate the Fourth Amendment because no privacy interest attaches to numbers that are only "a means of establishing communication." *Id.* Indeed, the Court noted that "[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." *Id.* (quotation omitted).

It follows that a search and seizure for Fourth Amendment purposes occurs in regard to electronic and telephonic communication when the government seeks to obtain communication content. *See id*. Because the information contained in packet-mode communications and post-cut-through digits reveals "the purport of any communication between the caller and the recipient of the call," *id.*, it is communication content entitled to the full protection of the Fourth Amendment.

There is no question that the *Order* requires carriers to provide communication content to law enforcement personnel. The *Order* explicitly states that its provision of packet-mode communications would allow law enforcement to access "both call-identifying information and call content even in cases where [law enforcement] is authorized only to receive call-identifying information (*i.e.*, under a pen register)." *Order*, ¶ 55. The *Order* also acknowledges that the standard it adopts for post-cut-through digits "permits[] [law enforcement] to access *non-call-identifying digits* (such as bank account numbers) with only a pen register warrant." *Order*, ¶ 123.

B. BECAUSE THE *ORDER* ALLOWS LAW ENFORCEMENT TO SEARCH AND SEIZE COMMUNICATION CONTENT, IT SHOULD BE VACATED.

Pursuant to the *Order*, law enforcement can search and seize call content in which an individual has a legitimate expectation of privacy.[38] Such action accordingly must comply with the requirements of the Fourth Amendment: law enforcement must obtain a warrant founded upon probable cause before obtaining that information.[39] Neither the traditional exceptions to the warrant requirement, nor the special needs exception to the Fourth Amendment's warrant requirement, apply to the electronic surveillance conducted by carriers pursuant to the *Order*.[40]

By its nature, electronic surveillance cannot be limited to a specific subject matter because it captures all of an individual's communications. Indeed, under the *Order*, law enforcement is unable to determine the subject of a communication until an interception has been completed. Thus, electronic surveillance pursuant to the *Order* has the potential to become precisely the sort of "dragnet" investigatory technique that the Fourth Amendment was designed to prohibit. Law enforcement's ability to utilize such inherently intrusive and broad means to search is limited by the stringent requirements of particularized suspicion, efficacy and need

---

[38] Though the Fourth Amendment typically applies only to searches or seizures by the government, when private actors, such as carriers, search or seize information at the direction of the government, they become agents or instruments of the government and must therefore comply with the dictates of the Fourth Amendment. *See Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 614 (1989). Like the railroads in *Skinner*, the carriers' actions are controlled by the Fourth Amendment because their searches and seizures are compelled by government regulations. *See id.* at 614-16.

[39] *See Dalia v. United States*, 441 U.S. 238, 256 n.18 (1979) (noting that warrant authorizing electronic surveillance complied with requirements of both Fourth Amendment and Title III).

[40] *See Chandler v. Miller*, 520 U.S. 305, 313-14 (1997) (explaining that special needs exception applies only when stated purpose of search is unrelated to law enforcement objectives); *Katz*, 389 U.S. at 357-58 (concluding that traditional exceptions to warrant requirement are inapplicable to electronic surveillance).

embodied by the Fourth Amendment's warrant requirement; it is this requirement that serves to prevent law enforcement overreaching.[41]

The *Order* allows communication content to be funneled to law enforcement upon only the most minimal showing of need, and it permits law enforcement to obtain call content information while avoiding the constitutional requirements constraining such collection. Indeed, as noted above, the Commission acknowledges that, pursuant to the *Order*, law enforcement officers will have access to certain content on the basis of only a pen register order. *See Order*, ¶ 123. Because the *Order* allows law enforcement access to such information without a showing of probable cause as determined by a neutral and detached magistrate, the *Order* mandates that carriers perform unconstitutional searches and seizures.[42] To the extent the *Order* authorizes such searches, it should be vacated.

C. THE COMMISSION'S UNCONSTITUTIONAL *ORDER* CAN NOT LEGITIMIZED BY INVOCATION OF THE EXCLUSIONARY RULE.

The Commission, recognizing that its *Order* implicates Fourth Amendment concerns, concluded that these unconstitutional searches are acceptable because the government's cannot use illegally seized evidence in court. *See Order*, ¶¶ 56, 123. An individual's Fourth Amendment rights are violated, however, not when government uses fruits of an illegal search, but rather, when the illegal search occurs.[43] The Commission cannot rely on a limited *remedy*

---

[41] *See Berger v. New York*, 388 U.S. 41, 58-59 (1967).

[42] *See Brown*, 50 F.3d at 294; *United States v. Lucht*, 18 F.3d 541, 546 (8th Cir. 1994) (holding that use of pen register to intercept call content violates Fourth Amendment and Title III).

[43] *See United States v. Balsys*, 524 U.S. 666, 692 (1998) ("breaches of privacy are complete at the moment of illicit intrusion, whatever use may or may not be made of their fruits"); *United States v. Verdugo-Urquidez*, 494 U.S. 259, 264 (1990) (explaining that Fourth Amendment prohibits unreasonable searches and seizures whether or not evidence is excluded from criminal trial because Fourth Amendment violation is "fully accomplished at the time of an unreasonable governmental intrusion").

for the unconstitutional seizure of evidence to validate an otherwise unconstitutional search. Such a concept is antithetical to the very purpose of the Fourth Amendment: to prevent government from overstepping its limited powers.

Any contention by the Commission that the exclusionary rule minimizes or rectifies the constitutional infirmity of its *Order* is simply unsupported by Fourth Amendment jurisprudence. Carried to its logical conclusion, such a contention would allow law enforcement to install a listening device in an individual's home without even a scintilla of suspicion, and for a completely illegitimate purpose such as harassment, so long as the evidence discovered thereby is not used in court against the individual. An important purpose of the exclusionary rule is *to deter future Fourth Amendment violations* by limiting the use of illegally seized evidence.[44] The exclusionary rule's evidentiary limitation in no way circumscribes the Fourth Amendment's protections or prevents its very application.[45]

---

[44] *See Arizona v. Evans*, 514 U.S. 1, 10 (1995).

[45] *See Verdugo-Urquidez*, 494 U.S. at 264.

CONCLUSION

For the foregoing reasons, the Court should vacate the *Order*.

Respectfully submitted,

Carlos Perez-Albuerne
Mark D. Cahill
Lawrence A. Friedman
Kathleen A. Burdette
CHOATE, HALL & STEWART
Exchange Place
53 State Street
Boston, Massachusetts 02109-2891
(617) 248-5000
Counsel for Petitioners

Kurt A. Wimmer
Gerard J. Waldron
Russell D. Jessee*
Margaret H. Grebe*
COVINGTON & BURLING
1201 Pennsylvania Avenue, N.W.
Washington, D.C. 20037
(202) 662-6000
Counsel for Petitioners

David L. Sobel, Esq.
Marc Rotenberg, Esq.
ELECTRONIC PRIVACY INFORMATION CENTER
666 Pennsylvania Avenue, S.E., Suite 301
Washington, D.C. 20003
Counsel for the Electronic Privacy Information Center

Shari Steele, Esq.
ELECTRONIC FRONTIER FOUNDATION
1550 Bryant Street, Suite 725
San Francisco, California 94103
Counsel for the Electronic Frontier Foundation

Barry Steinhardt, Esq.
AMERICAN CIVIL LIBERTIES UNION
125 Broad Street
New York, New York 10004
Counsel for the American Civil Liberties Union

** Members of the bars of Virginia and Wisconsin, respectively; not yet admitted in the District of Columbia*

Dated: January 20, 2000

CERTIFICATE OF SERVICE

I hereby certify that on this 20th day of January, 2000, I caused copies of the foregoing brief of the Public Interest Petitioners to be served on the parties indicated on the attached Service List by first-class, postage-prepaid United States mail.

_____

Kurt A. Wimmer

CERTIFICATE OF COMPLIANCE

I hereby certify on this 20th day of January, 2000, that the foregoing Brief of the Public Interest Petitioners complies with this Court's orders establishing the number of words to be contained in the brief of the Public Interest Petitioners.

_____

Kurt A. Wimmer

SERVICE LIST

Theodore B. Olson
Eugene Scalia
Montgomery N. Kosma
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, N.W., Suite 900
Washington, D.C. 20036-5303
Counsel for Petitioners Cellular Telecommunications Industry Association and Center for Democracy and Technology

John H. Harwood II
Lynn R. Charytan
Samir C. Jain
WILMER, CUTLER & PICKERING
2445 M Street, N.W.
Washington, D.C. 20037-1420
Counsel for Petitioner United States Telecom Association

Jerry Berman
James X. Dempsey
Center for Democracy and Technology
1634 Eye Street, N.W., Suite 1100
Washington, D.C. 20002
Counsel for Petitioner Center for Democracy and Technology

Michael Altschul
Cellular Telecommunications Industry Assoc.
1250 Connecticut Avenue, N.W., Suite 200
Washington, D.C. 20036
Counsel for Petitioner Cellular Telecommunications Industry Association

Lawrence E. Sarjeant
Linda L. Kent
Keith Townsend
United States Telecom Association
1401 H Street, N.W., Suite 600
Washington, D.C. 20036
Counsel for Petitioner United States Telecom Association

John E. Ingle
Deputy Associate General Counsel
Federal Communications Commission
445 Twelfth Street, S.W., Room 8-B201
Washington, D.C. 20554
Counsel for the Federal Communications Commission

Douglas N. Letter
Civil Division
U.S. Department of Justice
601 D Street, N.W., Room 9106
Washington, D.C. 20530
Counsel for the Department of Justice

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

Robert A. Long, Jr.
COVINGTON & BURLING
1201 Pennsylvania Avenue, N.W.
Washington, D.C. 20004
Counsel for Sprint PCS

Jonathan M. Chambers
Sprint PCS
Suite M-112
1801 K Street, N.W.
Washington, D.C. 20006
Counsel for Sprint PCS

Sylvia Lesse
John Kuykendall
KRASKIN, LESSE & COSSON
2120 L Street, N.W. - Suite 520
Washington, D.C. 20037
Counsel for Intervenor Rural Cellular Association

Grant Seiffert
Vice President, Government Relations
Matthew J. Flanigan, President
Telecommunications Industry Association
1300 Pennsylvania Avenue, N.W. - Suite 350
Washington, D.C. 20004
Counsel for Intervenor
Telecommunications Industry Association

Robert B. McKenna
Kathryn Marie Krause
1020 19th Street, N.W. - Suite 700
Washington, D.C. 20036
Counsel for Intervenor U S WEST, Inc.

Stewart A. Baker
Thomas M. Barba
L. Benjamin Ederington
Matthew L. Stennes
STEPTOE & JOHNSON, LLP
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036
Counsel for Intervenor
Telecommunications Industry Association