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

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

Mark D. Cahill
Lawrence M. Friedman
Kathleen A. Burdette
CHOATE, HALL & STEWART
Exchange Place
53 State Street
Boston, Massachusetts 02109-2891

(617) 248-5000 Counsel for Petitioners

Carlos Perez-Albuerne

Kurt A. Wimmer
Gerard J. Waldron
Russell D. Jessee*
Margaret H. Grebe*
COVINGTON & BURLING
1201 Pennsylvania Ave., N.W.
Washington, D.C. 20004
(202) 662-6000
Counsel for Petitioners
(Additional counsel listed on inside cover)

April 4, 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

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.

TABLE OF CONTENTS

I.		FRARY TO CONGRESS'S INTENT, THE ORDER PERMITS INTERCEPTION O INTERNET TRAFFIC	
Π.	ENFO	ORDER IMPROPERLY LOWERS THE STANDARD THAT LAW DRCEMENT MUST MEET TO CAPTURE THE CONTENT OF ELECTRONIC MUNICATIONS.	4
	A.	The Order Modifies Authorization Standards, Contrary To CALEA	5
	B.	Law Enforcement "Self-Policing" Does Not Validate The Order	6
III.		ENFORCEMENT CANNOT OBTAIN LOCATION INFORMATION AND POST THROUGH DIGITS WITH JUST A PEN REGISTER ORDER	
	A.	CALEA Does Not Transform Wireless Telephones Into Location Monitoring Devices.	9
	В.	The Commission's Order Unlawfully Allows Law Enforcement To Obtain Post-Cut-Through Digits Without A Title III Warrant	1

TABLE OF AUTHORITIES

CASES AND AGENCY DECISIONS

Adams Fruit Co. v. Barrett, 494 U.S. 638 (1990)	5
* Third Report and Order, In the Matter of Communications Assistance for Law Enforcement Act, CC Docket No. 97-213, FCC 99-230 (1999)	passim
Sanders v. Robert Bosch Corp., 38 F.3d 736 (4th Cir. 1994)	8
Smith v. Maryland, 442 U.S. 735 (1979)	5
United States v. Karo, 468 U.S. 705 (1984)	11
United States v Miller, 116 F.3d 641 (2d Cir. 1997)	7
CONSTITUTIONS AND STATUTES	
* Communications Assistance for Law Enforcement Act ("CALEA"), 47 U.S.C. § 1001 et seq.	passim
* Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. § 2510 et seq.	passim
* U.S. Const., amend. IV	passim
18 U.S.C. § 2703	3
18 U.S.C. § 3121(c)	6
47 U.S.C. § 271(c)(2)(B)(x)	10
47 U.S.C. § 325(b)(1)	11
OTHER MATERIALS	
H.R. Rep. No. 103-827, pt. 1 (1994)	3

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

GLOSSARY

American Civil Liberties Union ACLU: CALEA: Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified principally at 47 U.S.C. §§ 1001-1010) **Telecommunications Carriers Carriers**: CDT: Center for Democracy and Technology **Commission**: **Federal Communications Commission** CTIA: Cellular Telecommunications Industry Association DOJ: Department of Justice **Electronic Frontier Foundation** EFF: ECPA: Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified principally at 18 U.S.C. §§ 2701-2711 and 3121-3127) **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), reprinted in 1994 U.S.C.C.A.N. 3497. 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, Pub. L. No. 90-351, 82 Stat. 212 (1968) (codified principally at 18 U.S.C. §§ 2510-2520)

United States Telecom Association

USTA:

SUMMARY OF ARGUMENT

The privacy interests at stake in this proceeding – those of the American public in this age of new telecommunications technologies and of the Internet – are substantial. As currently written, the Commission's *Order* gives law enforcement access to highly sensitive and personal information that is protected by the Fourth Amendment and various statutes. In several instances, law enforcement's access will be overly broad and without meaningful safeguards. Moreover, the permitted invasions will be all the more insidious because it is unlikely that subjects of interceptions will ever know that their privacy has been violated. Aware of the potentially unlimited scope of electronic surveillance in the digital age, Congress recognized in CALEA that legitimate privacy interests should not be sacrificed for the sake of expediency. Congress built Fourth Amendment and Title III safeguards into CALEA, but the Commission in its *Order* has ignored them.

The government oversimplifies the Commission's *Order* by maintaining that CALEA is concerned only with access capabilities and does not require that certain protected information be turned over to law enforcement upon request. With respect to packet-mode communications, the *Order* seemingly permits law enforcement to reach the contents of packet-mode Internet communications including e-mail, a possibility that the government has not refuted. Moreover, the *Order* permits access to call content as well as call-identifying information when law enforcement only has a pen register order, which is contrary to the Commission's own analysis and in violation of the Fourth Amendment. The Court should not tolerate such a constitutional violation, even on an "interim" basis, and it should explicitly affirm that CALEA applies only to telephonic, not Internet, communications.

The *Order* gives law enforcement access to location information that Congress never intended to be available under CALEA, and this access – without the proper Title III authorization – constitutes a Fourth Amendment violation as well. At a minimum, the Court should confirm the necessity of a Title III warrant for obtaining location information. Finally, the *Order* permits law enforcement with only a pen register order to access post-cut-through digits that are call content, clearly violating Title III and Fourth Amendment protections. The Court should not allow this unjustified privacy invasion. Rather, it should establish that a Title III warrant is required for law enforcement to access call content. In all that they ask, Petitioners do not seek to hamstring legitimate law enforcement activity. Petitioners seek only the enforcement of the mandates found in CALEA and in the Constitution that law enforcement be required to follow procedures that guard the public's right to privacy.

ARGUMENT

I. CONTRARY TO CONGRESS'S INTENT, THE ORDER PERMITS INTERCEPTION OF ALL INTERNET TRAFFIC.

The Commission's *Order* defeats Congress's desire to exclude Internet service providers from CALEA's requirements by allowing law enforcement to intercept Internet traffic carried by the telecommunications carrier who transmits the Internet traffic. CALEA expressly excludes providers of "information services," such as Internet service providers, from the reach of its assistance requirements. See 47 U.S.C. §§ 1002(a), 1001(6), (8). Even though CALEA's requirements do not apply to telecommunications carriers "insofar as they are engaged in providing information services," 47 U.S.C. § 1001(8)(c)(i), the *Order* sweeps all packet-mode communications into its ambit.

The Commission erred when it failed to recognize the distinction, mandated by CALEA, between voice and data packet-mode communications. *See Order*, ¶ 54. The *Order* declares that "packet-mode communications, including call-identifying information and call content, may be delivered to law enforcement [with a pen register order] under the interim standard." *Order*, ¶ 55. By failing to specify that its requirements apply only to voice (or

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. . . . The 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, online service providers such as CompuServe, Prodigy, America-On-Line or Mead Data, or Internet service providers.

H.R. Rep. No. 103-827, at 18, 20 (1994) reprinted in 1994 U.S.C.C.A.N. 3498, 3500.

¹ As the House Report on CALEA explained:

² The government's position on the scope of the *Order* can only be implied from its silence when confronted with the issue. Nowhere in any of its briefs does the government challenge the apparent implications of the *Order*'s provisions authorizing interception of Internet traffic, which the Public Interest Petitioners addressed in their opening brief, *see* Pet'rs Brief, 6.

telephone) communications and not to data (or Internet) communications, the *Order* opens the door for law enforcement agencies to intercept and monitor e-mail and other Internet traffic with pen register orders. Such a result subverts the intent of Congress and accomplishes indirectly what Congress specifically forbade.

II. THE ORDER IMPROPERLY LOWERS THE STANDARD THAT LAW ENFORCEMENT MUST MEET TO CAPTURE THE CONTENT OF ELECTRONIC COMMUNICATIONS.

The *Order* modifies well-established standards for the interception of the content of electronic communications. CALEA itself does not change the authorization regime with which law enforcement must comply to intercept communication content. Rather, CALEA refers to a court order or "lawful authorization," thus emphasizing that the scope of the Commission's mandate is limited to delineation of interception *capabilities*. Despite the clear language of the statute, the Commission modified the level of *authorization* law enforcement must obtain before capturing call identifying information or communication content. Such modification of the existing authorization scheme incorporated in Title III and the pen-register statute, 18 U.S.C. § 2703, exceeds the Commission's mandate under CALEA and disturbs the careful balance Congress and the courts have struck between privacy interests and the needs of law enforcement.

The government attempts to avoid this fatal infirmity in two ways. First, the government maintains that the *Order* does not modify the existing authorization scheme contained in statutes like Title III. Second, the government argues that, in any event, law enforcement may capture communication content so long as law enforcement voluntarily separates communications content from call-identifying information to prevent the content from being viewed. Neither argument can salvage the *Order*.

A. The Order Modifies Authorization Standards, Contrary To CALEA.

While CALEA does not empower the Commission to modify the existing authorization regime, the unambiguous text of the *Order* does exactly that. *See* Pet'rs Brief, 7-9; *infra* Part III(B). The *Order* contemplates that carriers will provide communication content to law enforcement on the basis of only a pen register warrant or its equivalent – in other words, that law enforcement may in the future plausibly construe the *Order* as "lawful authorization" for the provision of this information. To the extent the *Order* so obligates the carriers, it transcends the limits on the provision of such information contemplated by the Fourth Amendment, *see Smith v. Maryland*, 442 U.S. 735, 741-42 (1979), and statutory authority like Title III and CALEA itself. Indeed, in decreeing that carriers must make communications content available to law enforcement on the basis of only a pen register warrant, the Commission has usurped the role of the courts and acted in an arena far outside its purview. Its judgment in such matters accordingly is entitled to no deference by this court on review. *See Adams Fruit Co. v. Barrett*, 494 U.S. 638, 649-50 (1990).

The Commission denies that the *Order* concerns anything but capabilities, and maintains that it reasonably evaluated and accounted for privacy interests in its *Order*. But the Commission's position is belied by the *Order* itself, which specifically discusses the standards under which certain communications content should be made available to law enforcement. *See Order*, ¶ 123. Given that the *Order* has been issued by the federal agency that directly regulates telecommunications carriers, it is very likely that these carriers will willingly comply with its mistaken standards. While law enforcement may be entitled to intercept call content in

appropriate circumstances, the Commission cannot alter the showing necessary to authorize such an interception.³

It is insufficient, moreover, for the government to recite vague assurances that law enforcement will ignore the Commission's *Order* and always seek the appropriate authorization in requesting carriers to provide intercepted information. *See* DOJ Brief, 3-5. Were law enforcement always to seek such authorization, there would never be any need to apply the exclusionary rule to protect the legitimate privacy rights of individuals against overzealous government investigators. Privacy protections should not and, constitutionally and statutorily, cannot depend upon the good intentions of the government's counsel. In addition, the protection of individuals' privacy rights should not devolve to telecommunications carriers, who, when faced with a surveillance demand by law enforcement under standards set by the very federal body that regulates them, simply will not be in a position to challenge the legal basis of those demands.

B. Law Enforcement "Self-Policing" Does Not Validate The Order.

DOJ grounds its "self-policing" defense of the *Order*'s packet-mode provision on 18 U.S.C. § 3121(c).⁴ *See* DOJ Brief, 16-18. The government contends that Section 3121(c) affirms its ability to intercept the entire content of packet-mode communications, in compliance

_

³ Furthermore, the government's contention that the interim nature of the *Order* somehow restores its legitimacy is incorrect. By adopting only an "interim" solution, the Commission nonetheless violates individuals' Fourth Amendment privacy interests and thus exceeded its mandate under CALEA. This "interim" period, moreover, may last for a substantial period of time – an entire year.

⁴ Section 3121(c) provides that "[a] government agency authorized to install and use a pen register under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing."

with both Title III and the Fourth Amendment, so long as law enforcement does not *look* at the content portion of intercepted packets. *See id.* This argument effectively eliminates the procedural safeguards surrounding Title III warrants. Title III and the Fourth Amendment require law enforcement to persuade a judge that there is probable cause to believe that an enumerated crime has been committed *before intercepting* the contents of surveillance targets' communications. The process of judicial application, and the rigorous procedural safeguards with which law enforcement must comply to obtain a warrant, exist to protect individual privacy and to prevent overreaching by law enforcement. By permitting the capture of individuals' communications on the lesser showing required to obtain a pen register order, and then relying on law enforcement to self-censor the information it seeks for investigative purposes, the *Order* operates from a premise that law enforcement may intercept communications *before* securing the necessary authorization – a result plainly at odds with Congressional intent and, of course, the requirements of the Fourth Amendment and Title III.

Although the government argues that the use of "minimizing technology" has been approved by the courts in conjunction with Title III, *see* DOJ Brief at 17, the cases cited by the government compel a contrary conclusion. In *United States v. Miller*, the court held only that "[a] pen register used merely to record the numbers dialed does not intercept the contents of a communication." 116 F.3d 641, 660 (2d Cir. 1997), *cert. denied*, 524 U.S. 905 (1998). The court acknowledged that if call content is intercepted, a Title III warrant is required; an interception, under the statute, may simply be the "*acquisition* of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4) (emphasis added). Under these standards, regardless of the technology employed, the intentional acquisition of call content requires compliance with Title

III – regardless of whether law enforcement actually *listens* to the call content. *See Sanders v. Robert Bosch Corp.*, 38 F.3d 736, 742 (4th Cir. 1994).

The Commission contends that, in the absence of available technology that can separate packet headers from packet content, it is unreasonable, and contrary to CALEA's purpose, "to prohibit carriers from delivering packets altogether, in disregard of the statutory requirement that carriers achieve the capability of delivering call-identifying information to duly authorized LEAs." FCC Brief, 40-41. The Commission fails to recognize that adopting an interim standard that unconstitutionally expands law enforcement's access to packet-mode communications violates the letter, and not merely the purpose, of CALEA. Even if CALEA specifically authorized the interception of all packet-mode communications on the authority of a pen register order – which it clearly does not – Congress cannot authorize the Commission to issue administrative orders that enlarge the constitutionally permissible bounds of electronic surveillance.

Finally, the government's claim that it has the technical ability to separate the content and header portions of packet-mode communications proves too much. The Commission concluded that such technology was *not* currently available to telecommunications carriers. *See Order*, ¶ 55. (If the government is correct, then the *Order* is, virtually by definition, arbitrary and capricious.) It was this very unavailability that served as the Commission's justification for mandating that telecommunications carriers provide entire packets to law enforcement. *See id*. And though the government professes that it would be satisfied if telecommunications carriers were able to deliver only the packet headers when surveillance was authorized by a pen register order, it offered no evidence of separation technology to the Commission. If separation technology is indeed available, telecommunications carriers should be required to use it when

law enforcement claims access to packet-mode communications on the basis of a pen register order. Requiring telecommunications carriers to deliver only packet headers to law enforcement is most consistent with the electronic surveillance capabilities of law enforcement before CALEA, provides the greatest protection for individual privacy, and is mandated by the Title III and the Fourth Amendment.

III. LAW ENFORCEMENT CANNOT OBTAIN LOCATION INFORMATION AND POST-CUT-THROUGH DIGITS WITH JUST A PEN REGISTER ORDER.

A. CALEA Does Not Transform Wireless Telephones Into Location Monitoring Devices.

The aspect of wireless telephones that makes them so attractive to consumers – mobility – also creates substantial privacy concerns when considered in the context of CALEA. Without proper safeguards, law enforcement could convert wireless telephones into location-monitoring devices. In the wireline world, law enforcement cannot track a person's movements based on a single telephone call. The only information they can glean (at least with a pen register order) is that someone at a home or business has picked up the phone and dialed a number. Simply because wireless telephones are mobile, there is no reason to allow law enforcement to contort CALEA to serve its own ends by turning wireless telephones into tracking devices.

The Commission's conclusion in its *Order* that a subject's cell site location is callidentifying information under CALEA – albeit information that is not available to law enforcement with only a pen register order – is unreasoned decisionmaking born out of an unsupportable compromise. The Commission perversely reasons that CALEA's express provision *excluding* location information from call-identifying information, *see* 47 U.S.C. § 1002(a)(2)(B), somehow provides a justification for *including* location information within

CALEA.⁵ The result of the Commission's logic is that location information is not callidentifying information when law enforcement has a pen register order but is magically transformed into call-identifying information when law enforcement has a Title III warrant. Location information either is or is not call-identifying information regardless of what authorization law enforcement is able to procure, and to hold otherwise is irrational.

The fundamental error in the Commission's *Order* and in the government's brief is that location information is not dialing or signaling information that identifies the origin or destination of a call. One has trouble divining from the Commission's conclusory statements why it believes that "a subject's cell site location at the beginning and end of a call identifies the 'origin' or 'destination' of a communication." *Order*, ¶ 44. Nonetheless, the Brief for the Telecommunications Petitioners cogently explains why the Commission's conclusion is factually inaccurate and inconsistent with CALEA. *See* Telecommunications Pet'rs Brief, 19-20. In the wireline environment, law enforcement obtains location information only incidentally because – as the Commission recognizes – "the telephone number usually corresponds with location." *Order*, ¶ 45. In the wireless environment, a telephone number only corresponds with a mobile telephone (and perhaps the user), but not with a fixed location. The location information that automatically passes between a mobile telephone and a cell site can in no way fit within a reasoned definition of "signaling information." That phrase clearly pertains to signals used to route calls, *see*, *e.g.*, 47 U.S.C. § 271(c)(2)(B)(x) (Communications Act referring to "signaling

_

⁵ Compare Order at ¶ 44 (citing as justification for including location information in callidentifying information provision: "with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices . . . call-identifying information shall not include any information that may disclose the physical location of the subscriber . . . "), with Telecommunications Pet'rs Brief at 21 (explaining Congress's reason for specific reference to pen registers and trap and trace devices).

necessary for call routing and completion"), and does not refer to any use of the electromagnetic spectrum, *see*, *e.g.*, 47 U.S.C. § 325(b)(1). Yet the briefs for the United States and the Commission deliberately confuse this key distinction. No rhetorical sleight-of-hand or conflation of distinct concepts can change the fact that for mobile telephones, call-identifying information does not include the location of a telephone's nearest cell site. The Commission's misinterpretation of call-identifying information cannot be sustained.

Despite the Commission's flawed reasoning on the definition of call-identifying information, the Commission correctly concluded that law enforcement cannot obtain location information merely with a pen register order. *Order*, ¶ 44. Indeed, the government concedes that "[a] pen register order does not by itself provide law enforcement with authority to obtain location information." DOJ Brief, 19; *see* FCC Brief, 36-37. Location information is, in some circumstances, constitutionally protected. *See United States v. Karo*, 468 U.S. 705, 714-15 (1984). In order to comply with both statutory and constitutional mandates, law enforcement needs the authorization of a Title III warrant to obtain location information. At a minimum, the Court should make explicit this limitation on law enforcement's ability under CALEA to obtain location information.

B. The Commission's Order Unlawfully Allows Law Enforcement To Obtain Post-Cut-Through Digits Without A Title III Warrant.

Individuals have a substantial interest in protecting the privacy of personal information such as bank account numbers, credit card numbers, and pager messages. Rhetoric about "capabilities" and "appropriate authorizations" aside, citizens should be aware that as a result of the Commission's *Order*, law enforcement will have access to this personal information with just a pen register order. The Commission itself recognizes the inherent danger and clearly concedes that some post-cut-through digits are call content. *See Order*, ¶ 119. Yet, despite some lip

service about "privacy implications," the Commission requires that a carrier deliver *all* post-cut-through digits to a law enforcement agency that has made the minimal showing necessary to procure a pen register order. *See id.*, ¶ 123.

Law enforcement's attempt to obtain call content with a pen register order cannot be justified by any argument about the breadth of the pen register statute. The government goes to great lengths to explain how the pen register statute allows law enforcement access to not only telephone numbers but also other forms of signaling information (for example, whether a phone is on or off the hook). *See* DOJ Brief, 7-8. But this is of no avail. A bank account number or credit card information cannot rationally be classified as "signaling information." Instead, this Court should determine that certain post-cut-through information is constitutionally protected content.

The Commission's *Order* provides no safeguard for this content. Complying with the safe harbor of the J-standard essentially is mandatory. Carriers have little choice but to view the J-standard as a *de facto* requirement (and no incentive to do otherwise) because the costs and potential penalties associated with trying to show that a response outside the safe harbor complies with CALEA are prohibitive. Thus, carriers will provide all post-cut-through digits to law enforcement agencies that have mere pen register orders, and the public is left with the vague, unenforceable assurances of law enforcement that it will "minimize" its interception by ignoring call content digits. In short, under the process decreed by the *Order*, a privacy violation is unavoidable. The only way for law enforcement to constitutionally obtain post-cut-through digits is through a Title III warrant. Any compromise on this safeguard, such as the one contained in the *Order*, cannot stand. But absent an explicit statement from the Court, law enforcement will have the imprimatur of the Commission to conduct unconstitutional searches.

CONCLUSION

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

Respectfully submitted,

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

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: April 4, 2000

Kurt A. Wimmer Gerard J. Waldron Russell D. Jessee* Margaret H. Grebe* COVINGTON & BURLING 1201 Pennsylvania Avenue, N.W. Washington, D.C. 20004 (202) 662-6000 Counsel for Petitioners

CERTIFICATE OF SERVICE

I hereby certify that on this 4th day of April, 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

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). Additionally, this brief complies with this Court's orders establishing the number of words to be contained in the reply brief of the Public Interest Petitioners. 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 3409 words.

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

STATUTORY ADDENDUM

All applicable statutes, etc., are contained in the Brief for the Telecommunications Petitioners.