U.S. Department of Justice

Criminal Division

Washington, D.C. 20530

CRM - 200601001F

DEC 18 2008

Marcia Hofmann
Staff Attorney
1875 Connecticut Avenue, NW
Suite 650
Washington, DC 20009

Dear Ms. Hofmann:

This is in response to your request of September 22, 2006, for access to records concerning all guidance issued; all inquiries; and all reports concerning the "content" of the pen register statute, 18 U.S.C. §§ 3121-3127.

We located records (items 1-42) in the Criminal Division within the scope of your request. We have processed your request under the Freedom of Information Act and will make all records available to you whose release is either required by that statute, or considered appropriate as a matter of discretion.

In light of our review, we have determined to release the enclosed items in full and to withhold certain items, as described on the enclosed schedule, in full. We are withholding the records indicated pursuant to one or more of the following FOIA exemptions set forth in 5 U.S.C. 552(b):

(5) which permits the withholding of inter-agency or intra-agency memorandums or letters which reflect the predecisional, deliberative processes of the Department, and/or which consist of attorney work product prepared in anticipation of litigation; and

(7) which permits the withholding of records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information...

(E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.

We found records originated by Office of Legislative Affairs. Pursuant to Department practice, we have referred these records to the originating offices for their review and direct response to you.

Also, we found records originated by the Office (or Offices) of an United States Attorney. Pursuant to Department practice, we have referred these records to the Executive Office for United States Attorneys (which processes such records) for its review and direct response to you.

You have a right to an administrative appeal of this partial denial of your request. Your appeal should be addressed to: The Office of Information and Privacy, United States Department of Justice, 1425 New York Ave., NW, Suite 11050, Washington, DC 20530-0001. Both the envelope and the letter should be clearly marked with the legend "FOIA Appeal." Department regulations provide that such appeals must be received by the Office of Information and Privacy within sixty days of the date of this letter. 28 C.F.R. 16.9. If you exercise this right and your appeal is denied, you also have the right to seek judicial review of this action in the federal judicial district (1) in which you reside, (2) in which you have your principal place of business, (3) in which the records denied are located, or (4) for the District of Columbia. If you elect to file an appeal, please include, in your letter to the Office of Information and Privacy, the Criminal Division file number that appears above your name in this letter.

Sincerely,

Rena Y. Kim

Rena Y. Kim, Chief
Freedom of Information/Privacy Act Unit
Office of Enforcement Operations
Criminal Division

Schedule of Records Withheld in Full
(Refer to Body of Letter for Full Description of Exemptions)

5. Draft document; 75 pages. Withheld pursuant to 5 U.S.C. 552(b)(5) and (7)(E).

6. Draft document, 140 pages. Withheld pursuant to 5 U.S.C. 552(b)(5) and (7)(E).

7. Draft Sealed Application with attachments, 45 pages. Withheld pursuant to 5 U.S.C. 552(b)(5).

8. Draft responses to Leahy 11/1 questions, 4 pages. Withheld pursuant to 5 U.S.C. 552(b)(5).

9. Documents depicting slides of presentation, 120 pages. Withheld pursuant to 5 U.S.C. 552(b)(5).

10. Draft Memorandum, 2/20/02, Martha Stansell-Gamm (Criminal Division) to Michael Chertoff (Assistant Attorney General); 80 pages. Withheld pursuant to 5 U.S.C. 552(b)(5).

11. Memorandum, Michael Chertoff (Assistant Attorney General) to Deputy Attorney General, 7 pages. Withheld pursuant to 5 U.S.C. 552(b)(5).

12. Memorandum, Martha Stansell-Gamm (Criminal Division) to Michael Chertoff (Assistant Attorney General); 5 pages. Withheld pursuant to 5 U.S.C. 552(b)(5).

13. Memorandum prepared by Richard W. Downing, 11/8/01; 2 pages. . Withheld pursuant to 5 U.S.C. 552(b)(5).

14. Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001, 14 pages. . Withheld pursuant to 5 U.S.C. 552(b)(5) and (7)(E).

15. Preliminary Analysts of the Computer Crime and Electronic Evidence Provisions of USA Patriot Act of 2001, 32 pages. Withheld pursuant to 5 U.S.C. 552(b)(5) and (7)(E).

16. Analysis of Sections of the USA Patriot Act of 2001 that relate to Computer Crime and Electronic Evidence, October, 2001, Richard Downing (Criminal Division); 84 pages. Withheld pursuant to 5 U.S.C. 552(b)(5) and (7)(E).

17. Analysis of Sections of the Anti-Terrorism Act of 2001 that relate to Computer Crime and Electronic Evidence, October, 2001, Richard Downing; 68 pages. Withheld pursuant to 5 U.S.C. 552(b)(5) and (7)(E).

18. Field Guidance on New Authorities Enacted in the 2001 Anti-Terrorism Legislation, 32 pages. Withheld pursuant to 5 U.S.C. 552(b)(5) and (7)(E).

19. Field Guidance on New Authorities (Redacted) Enacted in the 2001 Anti-Terrorism Legislation, 30 pages. Withheld pursuant to 5 U.S.C. 552(b)(5) and (7)(E).

20. Memorandum with attachments, Martha Stansell-Gamm (Criminal Division) to Michael Chertoff (Assistant Attorney General), 8 pages. Withheld pursuant to 5 U.S.C. (b)(5).

21. Memorandum, Michael Chertoff (Assistant Attorney General) to Deputy Attorney General; 9 pages. Withheld pursuant to 5 U.S.C. 552(b)(5).

22. Draft Memorandum, Larry D. Thompson (Deputy Attorney General), 5 pages. Withheld pursuant to 5 U.S.C. 552(b)(5).

23. Draft Memorandum, 5/14/02, Larry D. Thompson (Deputy Attorney General), 6 pages. Withheld pursuant to 5 U.S.C. 552(b)(5).

24. Draft, Field Guidance for the use of the Computer Tresoasser Exception to the Wiretap Statute, 18 U.S.C. Section 2511(2)(i);13 pages. Withheld pursuant to 5 U.S.C. 552(b)(5) and (7)(E).

25. Draft Memorandum, 9/23/02, Martha Stansell-Gamm (Criminal Division) to Dan Collins, (Associate Deputy Attorney General); 14 pages. Withheld pursuant to 5 U.S.C. 552(b)(5).

26. Memorandum with attachments, Martha Stansell-Gamm (Criminal Division) to Michael Chertoff (Assistant Attorney General); 7 pages. Withheld pursuant to 5 U.S.C. 552(b)(5).

27. Draft Memorandum, Michael Chertoff (Assistant Attorney General) to Deputy Attorney General, 12 pages. Withheld pursuant to 5 U.S.C. 552(b)(5).

28. Email with attachments, 7/18/02, Julie Samuels (Criminal Division) to Richard Downing (Criminal Division); 13 pages. Withheld pursuant to 5 U.S.C. 552(b)(5).

29. Draft Memorandum, Martha Stansell-Gamm (Criminal Division) to Michael Chertoff (Assistant Attorney General); 52 pages. Withheld pursuant to 5 U.S.C. 552(b)(5).

30. Comments on URL memo, 2 pages. Withheld pursuant to 5 U.S.C. 552(b)(5).

31. Draft documents, 2/3/02, Richard W. Downing; 25 pages. Withheld pursuant to 5 U.S.C. 552(b)(5).

32. Draft Memorandums, Martha Stansell-Gamm (Criminal Division) to Michael Chertoff (Assistant Attorney General); 54 pages. Withheld pursuant to 5 U.S.C. 552(b)(5).

33. Memorandum, 3/8/02, Andrew G. Oosterbaan (Criminal Division) to Julie Samuels (Criminal Division); 2 pages. Withheld pursuant to 5 U.S.C. 552(b)(5).

34. Draft Memorandums, Martha Stansell-Gamm (Criminal Division) to Michael Chertoff (Assistant Attorney General); 78 pages. Withheld pursuant to 5 U.S.C. 552(b)(5).

35. Draft Memorandum, Michael Chertoff (Criminal Division); 8 pages. Withheld pursuant to 5 U.S.C. 552(b)(5).

36. Memorandum, Michael Chertoff (Criminal Division) to Deputy Attorney General; 9 pages. Withheld pursuant to 5 U.S.C. 552(b)(5).

37. Memorandum with attachments, Martha Stansell-Gamm (Criminal Division) to Michael Chertoff (Assistant Attorney General); 3 pages. Withheld pursuant to 5 U.S.C. 552(b)(5).

38. Memorandum, Michael Chertoff (Assistant Attorney General) to Deputy Attorney General; 7 pages. Withheld pursuant to 5 U.S.C. 552(b)(5).

39. Draft Memorandums, 9/02; 33 pages. Withheld pursuant to 5 U.S.C. 552(b)(5).

40. Memorandum with attachments, Martha Stansell-Gamm (Criminal Division) to Michael Chertoff (Assistant Attorney General); 10 pages. Withheld pursuant to 5 U.S.C. 552(b)(5).

41. Emails; 73 pages. Withheld pursuant to 5 U.S.C. 552(b)(5).

42. Handwritten Note, 4 pages. Withheld pursuant to 5 U.S.C. 552(b)(5).

United States Court of Appeals,
District of Columbia Circuit.

UNITED STATES TELECOM ASSOCIATION, et al., Petitioners,
v.
FEDERAL COMMUNICATIONS COMMISSION and United States of America, Respondents.
AirTouch Communications, Inc., et al., Intervenors

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

Argued May 17, 2000.
Decided Aug. 15, 2000.

Telecommunications carriers and privacy rights organizations filed petitions for review challenging portions of Federal Communications Commission (FCC) order, 14 F.C.C.R. 16794, requiring carriers to implement technology enabling interception of information relating to wireless telephone calls under Communications Assistance for Law Enforcement Act (CALEA). Petitions were consolidated, and the Court of Appeals, Tatel, Circuit Judge, held that: (1) FCC failed to engage in reasoned decision-making in requiring dialed digit extraction, party hold/join/drop information, subject-initiated dialing and signaling information, and in-band and out-of-band signaling information; (2) technology that would make available locations of antenna towers used to connect at beginning and end of wireless telephone calls could be required as "call-identifying information;" and (3) FCC could require technology enabling interception of digital packet mode data.

Petitions granted in part and denied in part.

West Headnotes

[1] Statutes ⚿219(2)
361k219(2)

[1] Statutes ⚿219(4)
361k219(4)

To resolve a challenge to an agency's interpretation of a statute it is charged with administering, the court first determines whether Congress has directly spoken to the precise question at issue, and, if it has, that is the end of the matter, since the court, as well as the agency, must give effect to the unambiguously expressed intent of Congress; however, if the court finds the statute silent or ambiguous with respect to the precise question at issue, the court determines whether the agency's answer is based on a permissible construction of the statute, affording substantial deference to the agency's interpretation of statutory language.

[2] Telecommunications ⚿461.15
372k461.15

For purposes of *Chevron* analysis of Federal Communications Commission's (FCC) interpretation, Communications Assistance for Law Enforcement Act's (CALEA) definition of "call-identifying information," which included dialing or signaling information that identified origin, direction, destination, or termination of communication, was ambiguous as to whether it was limited to telephone numbers alone. Communications Assistance for Law Enforcement Act, § 102(2), 47 U.S.C.A. § 1001(2).

[3] Statutes ⚿195
361k195

Where Congress includes particular language in one section of a statute, but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion.

[4] Administrative Law and Procedure ⚿507
15Ak507

[4] Administrative Law and Procedure ⚿763
15Ak763

An agency must cogently explain why it has exercised its discretion in a given manner, and that explanation must be sufficient to enable the Court of Appeals to conclude that the agency's action was the product of reasoned decisionmaking.

[5] Telecommunications ⚿461.5
372k461.5

Federal Communications Commission (FCC) failed to engage in reasoned decisionmaking in requiring, under Communications Assistance for Law Enforcement Act (CALEA), telecommunications carriers to implement technology enabling post-cut-through dialed digit extraction, interception of party hold/join/drop information, interception of subject-initiated dialing and signaling information, including signals generated

by activating features such as call forwarding and call waiting, and interception of in-band and out-of- band signaling information; FCC simply concluded that required information was covered by CALEA's definition of "call-identifying information" without explaining how required information related to origin, direction, destination, or termination of calls, and FCC modified standards, which had been set by telecommunications industry association pursuant to CALEA, without identifying their deficiencies. Communications Assistance for Law Enforcement Act, §§ 102(2), 103(a)(2), 107(b), 47 U.S.C.A. §§ 1001(2), 1002(a)(2), 1006(b).

[6] Telecommunications ⚿461.5
372k461.5

Federal Communications Commission (FCC) acted arbitrarily and capriciously in requiring, under Communications Assistance for Law Enforcement Act (CALEA), that telecommunications carries implement call-identification technologies in addition to those established by telecommunications industry association (TIA) under CALEA, since FCC failed to ensure that CALEA's requirements were met by cost-effective methods and failed to ensure that cost of compliance on residential ratepayers was minimized; FCC adopted estimate predicting that TIA standards would cost $916 million and additional requirements would add $414 million, and then concluded without explanation that additional cost was not so exorbitant as to require exclusion, FCC made no attempt to determine cost of obtaining additional information through alternative methods, and FCC never explained impact on residential rates. Communications Assistance for Law Enforcement Act, §§ 103, 107(b)(1, 3), 47 U.S.C.A. §§ 1002, 1006(b)(1, 3).

[7] Administrative Law and Procedure ⚿763
15Ak763

Agency action must be based on a consideration of the relevant factors and must rest on reasoned decisionmaking in which the agency must examine the relevant data and articulate a satisfactory explanation for its action, including a rational connection between the facts found and the choice made.

[8] Telecommunications ⚿461.5
372k461.5

Federal Communications Commission (FCC) failed to adequately consider privacy and security of communications not authorized to be intercepted when it required, under Communications Assistance for Law Enforcement Act (CALEA), telecommunications carriers to implement post-cut-through dialed digit extraction technology capable of monitoring all digits dialed after calls were connected; although some post-cut-through digits were telephone numbers, others would convey call content, such as financial account numbers, passwords, and pager messages, and FCC rejected methods of allowing law enforcement agencies (LEAs) with only pen register orders to obtain phone numbers, but not call content, on ground that those methods would be costly and time consuming to LEAs. Communications Assistance for Law Enforcement Act, § 107(b)(1, 2), 47 U.S.C.A. § 1006(b)(1, 2).

[9] Telecommunications ⚿461.5
372k461.5

Federal Communications Commission (FCC) could require, pursuant to Communications Assistance for Law Enforcement Act's (CALEA's) definition of call-identifying information, telecommunications carriers to implement technology that would make available to law enforcement agencies (LEAs) locations of antenna towers that mobile phones used to connect at beginning and end of calls; call-identifying information included "signalling" information, mobile phones would send signal to nearest cell site at start and end of each call, location information LEAs would routinely obtain from telephone numbers in wireline environment was comparable to antenna tower location information in wireless environment, and LEAs would require something more than pen register order to obtain antenna location information. Communications Assistance for Law Enforcement Act, §§ 102(2), 103(a)(2), 47 U.S.C.A. §§ 1001(2), 1002(a)(2).

[10] Telecommunications ⚿461.5
372k461.5

Requirement under Communications Assistance for Law Enforcement Act (CALEA) that telecommunications carriers implement technologies that would enable law enforcement agencies (LEAs) to intercept digital packet mode data was proper, even though packet mode data would contain call content in addition to call- identifying packet header; since requirement was included in standards developed by telecommunications industry association (TIA), it was unaffected by any deficiencies in Federal Communications Commission's (FCC's) cost accounting, FCC recognized privacy concerns arising from requirement and asked TIA to study ways of separating header information from call content, and

LEAs would be required to obtain proper authorization before intercepting packet data from which call content had not been stripped. Communications Assistance for Law Enforcement Act, §§ 102(2), 103(a)(2), 107, 47 U.S.C.A. §§ 1001(2), 1002(a)(2), 1006.

***452 **280** On Petitions for Review of an Order of the Federal Communications Commission.

Theodore B. Olson argued the cause for petitioners United States Telecom Association, et al. With him on the briefs were Eugene Scalia, John H. Harwood, II, Lynn R. Charytan, Michael Altschul, Jerry Berman, James X. Dempsey, Lawrence E. Sarjeant, Linda L. Kent, John W. Hunter and Julie E. Rones.

***453 **281** Gerard J. Waldron argued the cause for petitioners Electronic Privacy Information Center, et al. With him on the briefs were Kurt A. Wimmer, Carlos Perez-Albuerne, Lawrence M. Friedman, Kathleen A. Burdette, David L. Sobel and Marc Rotenberg.

Stewart A. Baker, Thomas M. Barba, Matthew L. Stennes, Mary McDermott, Brent H. Weingardt, Todd B. Lantor, Robert A. Long Jr., Kevin C. Newsom, Robert B. McKenna and Dan L. Poole were on the brief for intervenor Sprint Spectrum, et al.

Philip L. Malet, William D. Wallace and William F. Adler were on the brief for intervenors Globalstar, et al.

John E. Ingle, Deputy Associate General Counsel, Federal Communications Commission, argued the cause for respondent Federal Communications Commission. With him on the brief were Christopher J. Wright, General Counsel, Laurence N. Bourne and Lisa S. Gelb, Counsel.

James M. Carr, Counsel, entered an appearance.

Scott R. McIntosh, Attorney, U.S. Department of Justice, argued the cause for respondent United States of America. With him on the brief were David W. Ogden, Acting Assistant Attorney General, and Douglas N. Letter, Attorney.

Before: GINSBURG, RANDOLPH and TATEL, Circuit Judges.

Opinion for the Court filed by Circuit Judge TATEL.

TATEL, Circuit Judge:

The Communications Assistance for Law Enforcement Act of 1994 requires telecommunications carriers to ensure that their systems are technically capable of enabling law enforcement agencies operating with proper legal authority to intercept individual telephone calls and to obtain certain "call- identifying information." In this proceeding, telecommunications industry associations and privacy rights organizations challenge those portions of the FCC's implementing Order that require carriers to make available to law enforcement agencies the location of antenna towers used in wireless telephone calls, signaling information from custom calling features (such as call forwarding and call waiting), telephone numbers dialed after calls are connected, and data pertaining to digital "packet-mode" communications. According to petitioners, the Commission exceeded its statutory authority, impermissibly expanded the types of call-identifying information that carriers must make accessible to law enforcement agencies, and violated the statute's requirements that it protect communication privacy and minimize the cost of implementing the Order. With respect to the custom calling features and dialed digits, we agree, vacate the relevant portions of the Order, and remand for further proceedings. We deny the petitions for review with respect to antenna tower location information and packet-mode data.

I

The legal standard that law enforcement agencies ("LEAs") must satisfy to obtain authorization for electronic surveillance of telecommunications depends on whether they seek to intercept telephone conversations or to secure a list of the telephone numbers of incoming and outgoing calls on a surveillance subject's line. In order to intercept telephone conversations, law enforcement agencies must obtain a warrant pursuant to Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Before issuing a Title III wiretap warrant, a judge must find that: (1) "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous"; and (2) there is probable cause for believing "that an individual is committing, has committed, or is about to commit" one of a list of specifically enumerated crimes, that the wiretap will intercept particular communications about the enumerated offense, and that the communications facilities to be tapped are either ***454 **282** being used in the commission of the crime or are commonly used by the suspect. 18 U.S.C. § 2518(3). The Electronic Communications Privacy Act of 1986 ("ECPA"), *id.* § 3121 *et seq.*, establishes less demanding standards for capturing telephone

numbers through the use of pen registers and trap and trace devices. Pen registers record telephone numbers of outgoing calls, *see id.* § 3127(3); trap and trace devices record telephone numbers from which incoming calls originate, much like common caller-ID systems, *see id.* § 3127(4). Although telephone numbers are not protected by the Fourth Amendment, *see Smith v. Maryland,* 442 U.S. 735, 742-45, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979), ECPA requires law enforcement agencies to obtain court orders to install and use these devices. Rather than the strict probable cause showing necessary for wiretaps, pen register orders require only certification from a law enforcement officer that "the information likely to be obtained is relevant to an ongoing criminal investigation." 18 U.S.C. § 3122(b)(2).

Wiretaps, pen registers and trap and trace devices worked well as long as calls were placed using what has come to be known as POTS, or "plain old telephone service." With the development and proliferation of new telecommunications technologies, however, electronic surveillance has become increasingly difficult. In congressional hearings, the FBI identified 183 "specific instances in which law enforcement agencies were precluded due to technological impediments from fully implementing authorized electronic surveillance (wiretaps, pen registers and trap and traces)." H.R. REP. NO.103-827, pt. 1, at 14-15 (1994). These impediments stemmed mainly from the limited capacity of cellular systems to accommodate large numbers of simultaneous intercepts as well as from the growing use of custom calling features such as call forwarding, call waiting, and speed dialing. *See id.* at 14.

Finding that "new and emerging telecommunications technologies pose problems for law enforcement," *id.,* Congress enacted the Communications Assistance for Law Enforcement Act of 1994 "to preserve the government's ability, pursuant to court order or other lawful authorization, to intercept communications involving advanced technologies such as digital or wireless transmission modes, or features and services such as call forwarding, speed dialing and conference calling, while protecting the privacy of communications and without impeding the introduction of new technologies, features, and services," *id.* at 9. Known as CALEA, the Act requires telecommunications carriers and equipment manufacturers to build into their networks technical capabilities to assist law enforcement with authorized interception of communications and "call- identifying information." *See* 47 U.S.C. § 1002. The Act defines "call- identifying information" as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier." *Id.* § 1001(2). CALEA requires each carrier to

> ensure that its equipment, facilities, or services ... are capable of
> (1) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission to or from the subscriber's equipment, facility, or service, or at such later time as may be acceptable to the government; [and]
> (2) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier....

***455 ****283** *Id.* § 1002(a)(1)-(2). Carriers must also " facilitat[e] authorized communications interceptions and access to call- identifying information ... in a manner that protects ... the privacy and security of communications and call-identifying information not authorized to be intercepted." *Id.* § 1002(a)(4)(A). Because Congress intended CALEA to "preserve the status quo," the Act does not alter the existing legal framework for obtaining wiretap and pen register authorization, "provid[ing] law enforcement no more and no less access to information than it had in the past." H.R. REP. NO. 103-827, pt. 1, at 22. CALEA does not cover "information services" such as e-mail and internet access. 47 U.S.C. §§ 1001(8)(C)(i), 1002(b)(2)(A).

To ensure efficient and uniform implementation of the Act's surveillance assistance requirements without stifling technological innovation, CALEA permits the telecommunications industry, in consultation with law enforcement agencies, regulators, and consumers, to develop its own technical standards for meeting the required surveillance capabilities. *See id.* § 1006. The Act "does not authorize any law enforcement agency or officer" to dictate the specific design of communications equipment, services, or features. *Id.* § 1002(b)(1). Although carriers failing to meet CALEA's requirements may incur civil fines of up to $10,000 a day, *see* 18 U.S.C. § 2522(c), the Act

establishes a safe harbor under which carriers that comply with the accepted industry standards will be deemed in compliance with the statute, *see* 47 U.S.C. § 1006(a)(2). But "if a Government agency or any other person believes that such requirements or standards are deficient, the agency or person may petition the Commission to establish, by rule, technical requirements or standards...." *Id.* § 1006(b). Such Commission rules must:

> (1) meet the assistance capability requirements of section 1002 of [the statute] by cost-effective methods;
> (2) protect the privacy and security of communications not authorized to be intercepted;
> (3) minimize the cost of such compliance on residential ratepayers;
> (4) serve the policy of the United States to encourage the provision of new technologies and services to the public; and
> (5) provide a reasonable time and conditions for compliance with and the transition to any new standard, including defining the obligations of telecommunications carriers under section 1002 of [the statute] during any transition period.

Id.

Following two years of proceedings and extensive negotiations with the FBI, the Telecommunications Industry Association ("TIA"), an accredited standard-setting body, adopted technical standards pursuant to CALEA's safe harbor, publishing them as Interim Standard/Trial Use Standard J-STD-025. Known as the "J-Standard," this document outlines the technical features, specifications, and protocols for carriers to make subscriber communications and call-identifying information available to law enforcement agencies having appropriate legal authorization.

Challenging the J-Standard as "deficient," *id.*, the Center for Democracy and Technology petitioned the Commission for a rulemaking to remove two provisions it claimed not only violate CALEA's privacy protections but also impermissibly expand government surveillance capabilities beyond those authorized by the statute. One of the challenged J-Standard provisions requires carriers to make available to law enforcement agencies the physical location of the nearest antenna tower through which a cellular telephone communicates at the beginning and end of a call. According to the Center, this requirement effectively converts ordinary mobile telephones into personal location-tracking devices, giving law enforcement agencies access to far more information than they ***456 **284** previously had. The Center also argued that cellular antenna location information is not "call-identifying information," as defined in both the statute and the J-Standard. The other challenged provision relates to what is known as "packet-mode data," which we shall describe in detail later in this opinion. *See* Section III *infra*. At this point, suffice it to say that, according to the Center, the J-Standard's inclusion of packet-mode data enables law enforcement agencies to obtain call content with no more than a pen register order.

Both the Justice Department and the FBI also petitioned the Commission to modify the J-Standard, arguing that it does not include all of CALEA's required assistance capabilities. The Department provided a list, known as the "FBI punch list," of nine additional surveillance capabilities that law enforcement wanted the Commission to add. The punch list included telephone numbers of calls completed using calling cards as well as signaling information related to custom calling features such as call waiting and conference calling.

After soliciting public comment on the petitions, *see* Public Notice, 13 F.C.C.R. 13786 (1998); Further Notice of Proposed Rulemaking 13 F.C.C.R. 22632 (1998), the Commission resolved the challenges to the J-Standard in its *Third Report & Order, see In the Matter of Communications Assistance for Law Enforcement Act,* 14 F.C.C.R. 16794 (1999) ("*Third Report & Order*"). The Commission denied the Center's petition to delete cellular antenna location information and packet-mode data. The location of cellular antenna towers used at the beginning and end of wireless calls, the Commission ruled, falls within CALEA's definition of call-identifying information because it "identifies the 'origin' or 'destination' of a communication." *Id.* at 16815 ¶ 44. With respect to packet-mode data, the Commission recognized the uncertainty regarding the technical feasibility of separating call content (requiring a Title III wiretap warrant) from call-identifying information (requiring only a pen register order). *See id.* at 16819-20 ¶¶ 55-56. Although inviting further study of the matter, the Commission declined to remove packet-mode data from the J-Standard, explaining that CALEA makes no distinction between packet-mode and other communications technologies. *See id.*

The Commission granted the Justice Department/FBI petition in part, adding four of the nine punch list capabilities to the J-Standard, adding two more in part (neither is challenged here), and declining to add three others (also unchallenged). *See id.* at 16852 ¶ 138.

The four added in full are:

(1) "Post-cut-through dialed digit extraction": This requires carriers to use tone-detection equipment to generate a list of all digits dialed after a call has been connected. Such digits include not only the telephone numbers dialed after connecting to a dial-up long-distance carrier (*e.g.,* 1-800-CALL-ATT), but also, for example, credit card or bank account numbers dialed in order to check balances or transact business using automated telephone services, *see id.* at 16842-46 ¶¶ 112-23;

(2) "Party hold/join/drop information": This includes telephone numbers of all parties to a conference call as well as signals indicating when parties are joined to the call, put on hold, or disconnected, *see id.* at 16825-28 ¶¶ 68- 75;

(3) "Subject-initiated dialing and signaling information": This includes signals generated by activating features such as call forwarding and call waiting, *see id.* at 16828-30 ¶¶ 76-82; and

(4) "In-band and out-of-band signaling": This includes information about signals sent from the carrier's network to a subject's telephone, such as message-waiting indicators, special dial tones, and busy signals, *see id.* at 16830-33 ¶¶ 83-89.

Two industry associations--the United States Telecom Association and the Cellular ***457 **285** Telecommunications Industry Association--joined by the Center for Democracy and Technology, filed a petition for review in this court, as did the Electronic Frontier Foundation, Electronic Privacy Information Center, and American Civil Liberties Union. All petitions were consolidated. The Telecommunications Industry Association, the standard- setting organization that developed and issued the J-Standard, joined by another trade group, the Personal Communications Industry Association, and two telecommunications carriers, Sprint PCS and U S West, intervened to challenge the *Third Report & Order,* focusing on dialed digit extraction, the most costly of the added punch list items. The FCC and the Justice Department filed separate briefs defending the Commission's action.

The consolidated petitions for review challenge six capabilities: antenna tower location information and packet-mode data, both of which were included in the J-Standard; and dialed digit extraction, party hold/join/drop, subject-initiated dialing and signaling, and in-band and out-of-band signaling, the four punch list capabilities added in full. With respect to these challenged capabilities, petitioners contend that the Commission: (1) exceeded its authority under CALEA because at least some of the information required to be made available to law enforcement is neither call content nor "call- identifying information that is reasonably available to the carrier," 47 U.S.C. § 1002(a)(2); (2) failed adequately to "protect the privacy and security of communications not authorized to be intercepted," as required by the statute, *id.* § 1006(b)(2); and (3) failed both to ensure that the capability requirements are implemented "by cost-effective methods," *id.* § 1006(b)(1), and to "minimize the cost of such compliance on residential ratepayers," *id.* § 1006(b)(3). In Section II, we take up the four challenged punch list capabilities and antenna tower location information. We consider packet-mode communications in Section III.

II

Whether CALEA requires carriers to make available antenna tower location information and the four punch list capabilities turns on what the Act means by "call-identifying information." To repeat, section 102(2) of CALEA defines "call-identifying information" as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier." *Id.* § 1001(2). The Commission interprets this definition to require adoption of all challenged capabilities, each of which, it claims, makes available information identifying the "origin, direction, destination, or termination" of calls. Petitioners argue that the definition limits "call-identifying information" to telephone numbers. Because location information and the four punch list items require carriers to make available more than telephone numbers, petitioners contend that these capabilities exceed CALEA's requirements. They argue that there is no statutory basis for location information to have been included in the J- Standard or for the Commission to have mandated the punch list capabilities.

[1] To resolve this challenge to the Commission's interpretation of a statute it is charged with administering, we proceed according to *Chevron U.S.A. Inc. v. Natural Resources Defense Council, Inc.,* 467 U.S. 837, 104 S.Ct. 2778, 81 L.Ed.2d 694 (1984). We ask first "whether Congress has directly spoken to the precise question at issue." *Id.* at 842, 104 S.Ct. 2778. If it has, "that is the end of the matter; for the court, as well as the agency, must give effect to the unambiguously expressed intent of Congress." *Id.* at 842-43, 104 S.Ct. 2778. If we find the statute silent

or ambiguous with respect to the precise question at issue, we proceed to the second step of *Chevron* analysis, asking "whether the agency's answer is based on a permissible ***458 **286** construction of the statute." *Id.* at 843, 104 S.Ct. 2778. At this stage of *Chevron* analysis, we afford substantial deference to the agency's interpretation of statutory language. *See id.* at 844, 104 S.Ct. 2778.

[2][3] Beginning with *Chevron* step one, we think it clear that section 102(2) does not "unambiguously" answer "the precise question at issue": Is "call-identifying information" limited to telephone numbers? To begin with, had Congress intended to so limit "call-identifying information," it could have done so expressly by using the term "telephone number" as it did in both sections 103(a)(2) and 207(a)(1)(C) of CALEA. *See* 47 U.S.C. § 1002(a)(2); 18 U.S.C. § 2703(c)(1)(C). "Where Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion." *Russello v. United States,* 464 U.S. 16, 23, 104 S.Ct. 296, 78 L.Ed.2d 17 (1983) (internal quotation marks and alteration omitted); *see also, e.g., District of Columbia Hosp. Ass'n v. District of Columbia,* 2000 WL 946581, at *3 (D.C.Cir.). CALEA's definition of "call-identifying information," moreover, refers not just to "dialing ... information," but also to "signaling information," leading us to believe that Congress may well have intended the definition to cover something more than just the "dialing ... information" conveyed by telephone numbers. Finally, section 103(a)(2) of CALEA provides that when information is sought pursuant to a pen register or trap and trace order, "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)." 47 U.S.C. § 1002(a)(2). As the Commission observed, Congress would have had no need to add this limitation if "call-identifying information" referred only to telephone numbers. *See Third Report & Order,* 14 F.C.C.R. at 16815 ¶ 44 n. 95.

In support of their argument that "call-identifying information" unambiguously means only telephone numbers, petitioners call our attention to the House Judiciary Committee Report, which does seem to describe such information in terms of telephone numbers. *See* H.R. REP. NO. 103-827, pt. 1, at 21. Apparently addressing post-cut-through dialed digits, the Report even says that "other dialing tones that may be generated by the sender that are used to signal customer premises equipment of the recipient are not to be treated as call-identifying information." *Id.* Yet the Report also echos CALEA's inherent ambiguity, stating that call-identifying information is "*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." *Id.* (emphasis added). Although another section of the Report describes CALEA as requiring carriers to make available "information identifying the originating and destination numbers of targeted communications, but not the physical location of targets," *id.* at 16, that passage, as the Commission points out, appears to deal with an earlier version of the statute--before the definition of "call-identifying information" was expanded by adding the terms "direction" and "termination."

Petitioners next argue that limiting "call-identifying information" to telephone numbers mirrors ECPA's definitions of "pen register" and "trap and trace device." Pen registers record "the *numbers* dialed or otherwise transmitted," 18 U.S.C. § 3127(3) (emphasis added), and trap and trace devices record "the originating *number* of ... an electronic communication," *id.* § 3127(4) (emphasis added). Petitioners contend that because CALEA's enforcement provisions are limited to intercept warrants and to pen register and trap and trace device orders, the statute's required capabilities must likewise be restricted ***459 **287** to the call content intercepted in a wiretap and the dialed telephone numbers recorded by pen registers. "It would have made no sense," say petitioners, "for Congress to require carriers to provide a capability that the surveillance laws do not authorize the government to use." Final Brief of Petitioners USTA, CTIA, and CDT at 16.

This is an interesting argument, but hardly sufficient to resolve CALEA's ambiguity. CALEA neither cross-references nor incorporates ECPA's definitions of pen registers and trap and trace devices. Moreover, the fact that CALEA's definition of "call-identifying information" differs from ECPA's description of the information obtainable by pen registers and trap and trace devices reinforces the statute's inherent ambiguity.

Petitioners also rely on the J-Standard's explanation of the terms used in CALEA's definition of call-identifying information, pointing out that the J-Standard limits these terms to telephone numbers:

> [D]estination is the number of the party to which a call is being made (e.g., called party); direction is the number to which a call is re-directed or the number from which it came, either incoming or outgoing (e.g., redirected-to party or redirected-from party); origin is the number of the party initiating a call (e.g., calling party); and termination is the number of the party ultimately receiving a call (e.g., answering party).

Interim Standard/Trial Use Standard J-STD-025, at 5. Because cell phone location information and the four challenged punch list capabilities call for more than telephone numbers, petitioners argue that they conflict with the J-Standard's interpretation of CALEA. Again, this is an interesting argument, but not relevant at *Chevron* step one, where our focus is on whether "the intent of *Congress* is clear." *Chevron,* 467 U.S. at 842, 104 S.Ct. 2778 (emphasis added). On that issue, the authors of the J-Standard can provide no guidance.

Finally, petitioners point out that in *Smith v. Maryland* the Supreme Court held that although the Fourth Amendment protects the privacy of information conveyed during telephone calls, *i.e.,* the contents of conversations, callers have no reasonable expectation of privacy in dialed telephone numbers. *See* 422 U.S. at 742-45, 95 S.Ct. 2427. Reading *Smith*'s exception narrowly, petitioners argue that other than call content interceptable under a wiretap order, CALEA cannot require carriers to provide law enforcement agencies anything more than the telephone numbers dialed in order to complete calls. But petitioners point to nothing in either CALEA or its legislative history to suggest that Congress meant to follow *Smith*'s protected-unprotected distinction in defining call-identifying information. Moreover, *Smith*'s reason for finding no legitimate expectation of privacy in dialed telephone numbers--that callers voluntarily convey this information to the phone company in order to complete calls--applies as well to much of the information provided by the challenged capabilities. *See id.* at 742, 99 S.Ct. 2577.

Turning to the government's position, we understand neither the Commission nor the Justice Department to be arguing that section 102(2) unambiguously includes more than telephone numbers in the definition of "call-identifying information," and for good reason. Although we reject petitioners' argument that section 102(2) is unambiguously limited to telephone numbers, we think it equally clear that nothing points to an "unambiguously expressed intent of Congress" to require every one of the challenged assistance capabilities. *Chevron,* 467 U.S. at 843, 104 S.Ct. 2778. Instead, the two agencies urge us to defer to the Commission's interpretation of the statute pursuant to *Chevron*'s second step. *See id.* at 844, 104 S.Ct. 2778. According to the agencies, the Commission reasonably interpreted "call-identifying information" to include the punch list capabilities and antenna tower location information. ***460 **288** Because we reach different conclusions with respect to the punch list and location information, we discuss them separately.

Punch List

Responding to the government's *Chevron*-two argument, petitioners contend: (1) the Commission's interpretation of "call-identifying information" to include the four added punch list capabilities is unreasonable and thus unworthy of *Chevron*-two deference; and (2) the Commission's decision to modify the J-Standard to include the punch list reflects a lack of reasoned decisionmaking, *see generally, Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co.,* 463 U.S. 29, 103 S.Ct. 2856, 77 L.Ed.2d 443 (1983). Because we agree with the latter argument, we need not address the Commission's plea for *Chevron* deference.

[4][5] It is well-established that " 'an agency must cogently explain why it has exercised its discretion in a given manner' and that explanation must be 'sufficient to enable us 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) (internal citation omitted) (quoting *Motor Vehicle Mfrs.,* 463 U.S. at 48, 52, 103 S.Ct. 2856). The Commission's determination that CALEA requires carriers to implement the four punch list items fails this test. The Commission *asserted* that each of the challenged punch list capabilities is required by CALEA because each requires carriers to make available "call-identifying information," but it never explained--not in the Order and not in its brief--the basis for this conclusion. Nowhere in the record did the Commission explain how the key statutory terms--origin, direction, destination, and termination--can cover the wide variety of information required by the punch list. For example, the Commission uses "origin" of a communication to mean not only the telephone number of an incoming call, but also a tone indicating that a new call is waiting. Adding the waiting call to create a three-way call is yet another origin. If a party is placed on hold and then re-joined to the call, the Commission describes that event as "the temporary origin ... of a communication." *Third Report & Order,* 14 F.C.C.R. at 16827 ¶ 74. The

Commission similarly uses "termination" to cover many different kinds of information including telephone numbers of outgoing calls, signals indicating that calls have been placed on hold or switched to waiting calls, signals that parties have been dropped from conference calls, busy signals, and ringing tones. Yet the Commission never explained how each of these bits of information "*identifies the ... termination* of each communication." 47 U.S.C. § 1001(2) (emphasis added). Instead, it simply concluded, with neither analysis nor explanation, that each capability is required by CALEA. *See, e.g., Third Report & Order,* 14 F.C.C.R. at 16827 ¶ 74 ("Party 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." (emphasis added)).

Perhaps the Commission can satisfactorily explain how CALEA's terms can encompass such a wide range of information. Because it has not, we cannot tell whether the punch list capability requirements are "the product of reasoned decisionmaking." *Motor Vehicle Mfrs.,* 463 U.S. at 52, 103 S.Ct. 2856.

The Commission's failure to explain its reasoning is particularly serious in view of CALEA's unique structure. Rather than simply delegating power to implement the Act to the Commission, Congress gave the telecommunications industry the first crack at developing standards, authorizing the Commission to alter those standards only if it found them "deficient." 47 U.S.C. § 1006(b). Although the Commission used its rulemaking power to alter the J-Standard, it identified no deficiencies in ***461 **289** the Standard's definitions of the terms "origin," " destination," "direction," and "termination," which describe "call-identifying information" in terms of telephone numbers. Were we to allow the Commission to modify the J-Standard without first identifying its deficiencies, we would weaken the major role Congress obviously expected industry to play in formulating CALEA standards.

The Commission's decision to include the four challenged punch list capabilities suffers from two additional defects. The first relates to CALEA's requirements that Commission rules must "meet the assistance capability requirements of section 1002 of this title by cost-effective methods" and "minimize the cost of such compliance on residential ratepayers." *Id.* § 1006(b)(1), (3). Faced with multiple cost estimates ranging as high as $4 billion for all carriers to implement the core J-Standard capabilities, the Commission adopted an estimate submitted by five software suppliers predicting that they would earn $916 million in revenues for implementing the core J-Standard and $414 million for implementing the punch list. *Third Report & Order,* 14 F.C.C.R. at 16805 ¶ 20, 16809 ¶ 30. The Commission acknowledged that "these estimates ... do not represent all carrier costs of implementing CALEA," *id.* at 16809 ¶ 30, yet it found them to be "a reasonable guide of the costs to wireline, cellular, and broadband PCS carriers for CALEA compliance," *id.*

[6] The Commission never explained how its Order would satisfy CALEA's requirements "by cost-effective methods." 47 U.S.C. § 1006(b)(1). It made no attempt to compare the cost of implementing the punch list capabilities with the cost of obtaining the same information through alternative means, nor did it explain how it measured cost-effectiveness. Although it mentioned residential ratepayers, it never explained what impact its Order would have on residential telephone rates. Instead, pointing out that the telecommunications industry, by ratifying the J-Standard, had agreed to its implementation cost, the Commission compared the additional cost of each punch list capability with the total cost of the J-Standard and then concluded that each additional cost was "not so exorbitant as to require automatic exclusion of the capability." *Third Report & Order,* 14 F.C.C.R. at 16824 ¶ 66, 16828 ¶ 75, 16829-30 ¶ 82, 16832 ¶ 89. But why? The Commission failed to explain how it decided that implementing the punch list capabilities, which increase J- Standard costs by more than 45 percent (even by the Commission's conservative estimates) is "not so exorbitant." Suppose punch list costs had exceeded J- Standard costs by 90 percent. Would that have been too "exorbitant"? Asked this question at oral argument, Commission counsel told us only, "I suppose it is a line-drawing exercise."

[7] The Commission's response to CALEA's cost directives reflects a classic case of arbitrary and capricious agency action. Fundamental principles of administrative law require that agency action be "based on a consideration of the relevant factors," *Citizens to Preserve Overton Park, Inc. v. Volpe,* 401 U.S. 402, 416, 91 S.Ct. 814, 28 L.Ed.2d 136 (1971), and rest on reasoned decisionmaking in which "the agency must examine the relevant data and articulate a satisfactory explanation for its action including a rational connection between the facts found and the choice made," *Motor Vehicle Mfrs.,* 463 U.S. at 43, 103 S.Ct.

2856 (internal quotation marks omitted). Of course, we do not require "ideal clarity"; we will "uphold a decision ... if the agency's path may reasonably be discerned." *Bowman Transp., Inc. v. Arkansas-Best Freight System Inc.,* 419 U.S. 281, 286, 95 S.Ct. 438, 42 L.Ed.2d 447 (1974). On the record before us, however, we cannot "discern" how the Commission interpreted "cost-effective," nor why it considered the substantial costs of the punch list capabilities to be "not so exorbitant," nor finally what impact it thought the Order would have on residential**462 **290** ratepayers. Missing, in other words, is "a rational connection between the facts found and the choice made." *Motor Vehicle Mfrs.,* 463 U.S. at 43, 103 S.Ct. 2856.

[8] The second defect in the Order relates to the Commission's failure to comply with CALEA's requirement that it "protect the privacy and security of communications not authorized to be intercepted," 47 U.S.C. § 1006(b)(2), with respect to post-cut-through dialed digit extraction. This punch list capability requires carriers to monitor electronically the communications channel that carries audible call content in order to decode all digits dialed after calls are connected or "cut through." Some post-cut-through dialed digits are telephone numbers, such as when a subject places a calling card, credit card, or collect call by first dialing a long-distance carrier access number and then, after the initial call is "cut through," dialing the telephone number of the destination party. Post-cut-through dialed digits can also represent call content. For example, subjects calling automated banking services enter account numbers. When calling voicemail systems, they enter passwords. When calling pagers, they dial digits that convey actual messages. And when calling pharmacies to renew prescriptions, they enter prescription numbers.

The government contends that a law enforcement agency may receive all post- cut-through digits with a pen register order, subject to CALEA's requirement that the agency uses "technology reasonably available to it" to avoid processing digits that are content. 18 U.S.C. § 3121(c). No court has yet considered that contention, however, and it may be that a Title III warrant is required to receive all post-cut-through digits. The Commission therefore had a statutory obligation to address how its Order, which requires the capability to provide all dialed digits pursuant to a pen register order, would "protect the privacy and security of communications not authorized to be intercepted." 47 U.S.C. § 1006(b)(2). The Commission spoke of law enforcement's need to obtain post-cut-through dialed digits and of the cost of providing them, but it never explained, as CALEA requires, how its rule will "protect the privacy and security of communications not authorized to be intercepted."

Several commenters, moreover, suggested ways in which law enforcement agencies having only pen register orders could obtain post-cut-through phone numbers while protecting the privacy of call content. The Commission rejected these alternatives, claiming not that they are technologically infeasible, but that they "would shift the cost burden from the originating carrier to the LEA," "could be time-consuming," and might burden law enforcement's ability "to conduct electronic surveillance effectively and efficiently." *Third Report & Order,* 14 F.C.C.R. at 16845 ¶ 121. This is an entirely unsatisfactory response to CALEA's privacy provisions. The statute requires the Commission to consider more than the burden on law enforcement--after all, any privacy protections burden law enforcement to some extent. The Commission's rules must not only meet CALEA's "assistance capability requirements," 47 U.S.C. § 1006(b)(1), but also "protect the privacy and security of communications not authorized to be intercepted," *id.* § 1006(b)(2).

The absence of any meaningful consideration of privacy with respect to dialed digit extraction does not seem to stem from a failure on the Commission's part to understand the privacy consequences of its Order. To the contrary, recognizing that there is no way to distinguish between digits dialed to route calls and those dialed to communicate information, the Commission expressed "concern[ ] about ... the privacy implications of permitting LEAs to access non-call-identifying digits (such as bank account numbers) with only a pen register warrant." *Third Report & Order,* 14 F.C.C.R. at 16846 ¶ 123. Yet the Order requires carriers to make available all post-cut-through dialed digits--those that ***463 **291** convey content as well as telephone numbers.

Asked at oral argument to point out how the Commission applied CALEA's privacy mandate to post-cut-through dialed digits, Commission counsel stated, "we addressed ourselves to the privacy questions with a little bit of hand wringing and worrying...." Transcript of Oral Argument at 29. Neither hand wringing nor worrying can substitute for reasoned decisionmaking.

For the foregoing reasons, we vacate the portions of

the Commission's Order dealing with the four challenged punch list capabilities and remand for further proceedings consistent with this opinion.

Location Information

[9] We reach a different conclusion with respect to the Commission's refusal to remove the antenna tower location information capability from the J- Standard. This provision requires carriers to make available the physical location of the antenna tower that a mobile phone uses to connect at the beginning and end of a call. Unlike the Commission's adoption of the punch list, its decision with regard to location information is both reasoned and reasonable.

To begin with, as the Commission observed in the *Third Report & Order,* defining "call-identifying information" to include antenna tower location finds support in CALEA's text. In particular, section 103(a)(2) provides that "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 (except to the extent that the location may be determined from the telephone number)." 47 U.S.C. § 1002(a)(2). As we note above, the Commission read this provision to imply that location information falls within the definition of call-identifying information. Section 103(a)(2), the Commission ruled, "simply imposes upon law enforcement an authorization requirement different from that minimally necessary for use of pen registers and trap and trace devices." *Third Report & Order,* 14 F.C.C.R. at 16815 ¶ 44. Disagreeing, petitioners argue that section 103(a)(2) narrows the definition of call-identifying information and should not be read as an affirmative grant of authority for law enforcement agencies to obtain location information. As the Commission explained, however, if "call-identifying information" did not include location information, this provision would have no function. *See id.* at 16815 ¶ 44 & n. 95. In reaching this conclusion, the Commission was simply following the well-accepted principle of statutory construction that requires every provision of a statute to be given effect. *See Washington Market Co. v. Hoffman,* 101 U.S. (11 Otto) 112, 115-16, 25 L.Ed. 782 (1879) ("We are not at liberty to construe any statute so as to deny effect to any part of its language.").

The Commission's approach to location information also finds support in CALEA's use of the word "signaling" in the definition of "call-identifying information." As the agency explains in its brief, a mobile phone "sends signals to the nearest cell site at the start and end of a call. These signals, which are necessary to achieve communications between the caller and the party he or she is calling, clearly are 'signaling information.' Information about the cell sites associated with mobile calls therefore falls squarely within the statutory definition of call-identifying information." Brief for Federal Communications Commission at 38.

Not only did the Commission elucidate the textual basis for interpreting "call-identifying information" to include location information, but it also explained how that result comports with CALEA's goal of preserving the same surveillance capabilities that law enforcement agencies had in POTS (plain old telephone service). "[I]n the wireline environment," the Commission ***464 ****292** explained, law enforcement agencies "have generally been able to obtain location information routinely from the telephone number because the telephone number usually corresponds with location." *Third Report & Order,* 14 F.C.C.R. at 16816 ¶ 45. In the wireless environment, "the equivalent location information" is "the location of the cell sites to which the mobile terminal or handset is connected at the beginning and at the termination of the call." *Id.* Accordingly, the Commission concluded, "[p]rovision of this particular location information does not appear to expand or diminish law enforcement's surveillance authority under prior law applicable to the wireline environment." *Id.*

The Commission's refusal to remove location information from the J-Standard, moreover, does not share the other problems that led us to vacate the punch list portion of the *Third Report & Order.* As to cost, location information was included in the J-Standard adopted by industry, so it is unaffected by the deficiencies in the Commission's cost analysis. And in contrast to dialed digit extraction, the Commission's analysis of the location capability did more than just pay lip service to CALEA's privacy requirements. Most important, the Commission demonstrated its understanding that antenna location information could only be obtained with something more than a pen register order, *see id.* at 16815 ¶ 44, a point the Justice Department concedes in its brief: "A pen register order does not by itself provide law enforcement with authority to obtain location information, and we have never contended otherwise." Final Brief for the United States at 19. Expressly relying on CALEA's privacy protection provisions, moreover, the Commission rejected a New York Police Department

proposal that would have required triangulating signals from multiple cellular antenna towers to pinpoint a wireless phone's precise location throughout a call's duration. *See Third Report & Order,* 14 F.C.C.R. at 16816 ¶ 46. "[S]uch a capability," the Commission found, "poses difficulties that could undermine individual privacy." *Id.*

For these reasons, we deny the petitions for review with respect to location information.

III

[10] This brings us to petitioners' challenge to the Commission's decision not to remove the packet-mode data requirement from the J-Standard. In conventional circuit-mode telecommunications, a single circuit is opened between caller and recipient and all electronic signals that make up the communication travel along the circuit. In digital packet-switched networks, communications do not travel along a single path. Instead, a call is broken into a number of discrete digital data packets, each traveling independently through the network along different routes. Data packets are then reassembled in the proper sequence at the call's destination. Like an envelope, each digital packet has two components: it contains a portion of the communication message, and it bears an address to ensure that it finds its way to the correct destination and is reassembled in proper sequence. The address information appears in the packet's "header." The message within the packet is known as the "body" or "payload." The J-Standard requires that carriers make available both header and payload.

Telecommunication carrier petitioners claim that packet headers (call- identifying information) cannot be separated from packet bodies or payloads (call content). Accordingly, they and the privacy petitioners argue that any packet-mode data provided to a law enforcement agency pursuant to a pen register order will inevitably include some call content, thus violating CALEA's privacy protections. The FBI disagrees. "[A]s a technical matter," it argued before the Commission, "it is perfectly feasible for a LEA to employ equipment that distinguishes between a packet's header and its communications payload and makes only the relevant header information***465 **293** available for recording or decoding." *Third Report & Order,* 14 F.C.C.R. at 16818 ¶ 54.

The Commission considered these conflicting views about the feasibility of separating call content from packet header data, concluding that "the record is not sufficiently developed to support any particular technical requirements for packetmode communications." *Id.* at 16817 ¶ 48. At the same time, the Commission acknowledged that "privacy concerns could be implicated if carriers were to give to LEAs packets containing both call-identifying and call content information when only the former was authorized." *Id.* Stating 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 Telecommunications Industry Association, which developed the J-Standard, "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.* at 16819 ¶ 55. In the meantime, however, finding the record insufficient to warrant modification of the J-Standard's packet-mode data provision, the Commission directed that it be implemented "no later than September 30, 2001." *Id.* "That date," the Commission explained, "is 15 months after the June 30, 2000 CALEA compliance deadline, and will afford manufacturers that have not yet developed a packet-mode capability the time needed to do so." *Id.* At the same time, the Commission emphasized that it viewed this as an interim solution. "We recognize that, in view of the growing importance of packet-mode communications, a timely permanent solution is essential. Accordingly, we expect that TIA will deliver a report to us no later than September 30, 2000 that will detail a permanent solution...." *Id.* at 16820 ¶ 56.

The Commission's denial of the petitions to remove packet-mode data from the J-Standard suffers from none of the shortcomings that undermined its handling of the punch list capabilities. First, because nobody questions that packet header information contains "call-identifying information," the ambiguity of that term's definition does not affect the packet-mode requirement. Second, as with location information, but unlike the four punch list capabilities, because the packetmode requirement was included in the J-Standard adopted by industry it is unaffected by the deficiencies in the Commission's cost analysis. Third, unlike the case of dialed digit extraction, the Commission thoroughly considered the privacy implications of packet-mode data and invited further study to "better address privacy concerns." *Id.* at 16819 ¶ 55.

Finally, nothing in the Commission's treatment of packet-mode data requires carriers to turn over call content to law enforcement agencies absent lawful

authorization. Although the Commission appears to have interpreted the J-Standard as expanding the authority of law enforcement agencies to obtain the contents of communications, *see id.,* the Commission was simply mistaken. All of CALEA's required capabilities are expressly premised on the condition that any information will be obtained "pursuant to a court order or other lawful authorization." 47 U.S.C. § 1002(a)(1)-(3). CALEA authorizes neither the Commission nor the telecommunications industry to modify either the evidentiary standards or procedural safeguards for securing legal authorization to obtain packets from which call content has not been stripped, nor may the Commission require carriers to provide the government with information that is "not authorized to be intercepted." *Id. See also* Final Brief for the United States at 4 ("If the government lacks the requisite legal authority to obtain particular information, nothing in Section 103 obligates a carrier to provide such information."). Petitioners thus have no reason to fear ***466 **294** that "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.' " Final Brief of Petitioners USTA, CTIA, and CDT at 35. We therefore deny the petition for review with respect to packet-mode data.

IV

We grant the petitions for review in part, vacate the provisions of the *Third Report & Order* dealing with the four challenged punch list capabilities, and remand to the Commission for further proceedings consistent with this opinion. In all other respects, we deny the petitions for review.

So ordered.

227 F.3d 450, 343 U.S.App.D.C. 278, 20 Communications Reg. (P&F) 1285

END OF DOCUMENT

Date of Printing: NOV 13,2003

KEYCITE

ITATION: **U.S. Telecom Ass'n v. F.C.C., 227 F.3d 450, 343 U.S.App.D.C. 278 (D.C.Cir., Aug 15, 2000) (NO. 99-1442,)-1523, 99-1466, 99-1475)**

History
Direct History

> 1 **U.S. Telecom Ass'n v. F.C.C.,** 227 F.3d 450, 343 U.S.App.D.C. 278 (D.C.Cir. Aug 15, 2000) (NO. 99-1442, 99-1523, 99-1466, 99-1475)

On Remand to

2 In re Communications Assistance For Law Enforcement Act, 2002 WL 534605, 17 F.C.C.R. 6896, 17 FCC Rcd. 6896 (F.C.C. Apr 11, 2002) (NO. FCC 02-108, 97-213)

KEYCITE

ITATION: **U.S. Telecom Ass'n v. F.C.C., 227 F.3d 450, 343 U.S.App.D.C. 278 (D.C.Cir., Aug 15, 2000) (NO. 99-1442, 9-1523, 99-1466, 99-1475)**

Citing References

Positive Cases (U.S.A.)

**** Cited**

1 Sprint Corp. v. F.C.C., 331 F.3d 952, 958, 356 U.S.App.D.C. 367 (D.C.Cir. Jun 17, 2003) (NO. 02-1129)

2 U.S. Telecom Ass'n v. F.B.I., 276 F.3d 620, 622, 349 U.S.App.D.C. 277, 279 (D.C.Cir. Jan 18, 2002) (NO. 00-5386) **HN: 8 (F.3d)**

3 AT&T Wireless Services, Inc. v. F.C.C., 270 F.3d 959, 968, 348 U.S.App.D.C. 135 (D.C.Cir. Nov 09, 2001) (NO. 00-1304) "" **HN: 7 (F.3d)**

4 In re Verizon Internet Services, Inc., 240 F.Supp.2d 24, 31, 2003 Copr.L.Dec. P 28,580, 28580, 65 U.S.P.Q.2d 1574, 1574 (D.D.C. Jan 21, 2003) (NO. CIV.A.02-MS-0323(JDB) "" **HN: 1 (F.3d)** (BNA Version)

*** Mentioned**

5 Kentucky Resources Council, Inc. v. Norton, 2002 WL 1359455, *2, 37 Fed.Appx. 545, 548 (D.C.Cir. May 30, 2002) (Table, text in WESTLAW, NO. 01-5263) **HN: 4 (F.3d)**

6 National Mining Ass'n v. Chao, 160 F.Supp.2d 47, 77 (D.D.C. Aug 09, 2001) (NO. CIV. 00-3086(EGS)) **HN: 4,7 (F.3d)**

7 Walton v. Safir, 122 F.Supp.2d 466, 478, 80 Empl. Prac. Dec. P 40,634, 40634, 17 IER Cases 49, 49 (S.D.N.Y. Nov 27, 2000) (NO. 99 CIV. 4430 (AKH)) **HN: 8 (F.3d)**

Administrative Decisions (U.S.A.)

8 The Common Carrier and Wireless Telecommunications Bure au, 2001 WL 1142170, *6, 16 F.C.C.R. 17,101, 16 FCC Rcd. 17,101 (F.C.C. Sep 28, 2001) (NO. DA 01-2243) ** **HN: 10 (F.3d)**

9 In re Communications Assistance for Law Enforcement Act, 2001 WL 1104564, *8+, 16 F.C.C.R. 17,397+, 16 FCC Rcd. 17,397+ (F.C.C. Sep 21, 2001) (NO. FCC 01-265, CC 97-213) "" *** **HN: 10 (F.3d)**

10 In re Communications Assistance for Law Enforcement Act, 2001 WL 370181, *13, 16 F.C.C.R. 8959, 16 FCC Rcd. 8959 (F.C.C. Apr 16, 2001) (NO. FCC 01-126, CC 97-213) *

11 In re Communications Assistance for Law Enforcement Act, 2000 WL 1744634, *1, 15 F.C.C.R. 23,776, 15 FCC Rcd. 23,776 (F.C.C. Nov 29, 2000) (NO. CC 97-213, DA 00-2683) **

12 In re Commission Seeks Comments to Update Record in Calea Technical Capabilities Proceeding, 2000 WL 1528264, *1, 15 F.C.C.R. 20,142, 15 FCC Rcd. 20,142 (F.C.C. Oct 17, 2000) (NO. CC 97-213, DA 00-2342) ** **HN: 4 (F.3d)**

Registers (U.S.A.)

13 Communications Assistance for Law Enforcement Act, 67 Federal Register 21999 (May 02, 2002) ** **HN: 5,8 (F.3d)**

Secondary Sources (U.S.A.)

14 Civ. Actions Against US, Agencies, Officers & Empl. s 6:35, REVIEW ON RECORD (2002) **HN: 4 (F.3d)**

Citing References

Secondary Sources (U.S.A.)

15 Tax Fraud & Evasion 14.02, FOURTH AMENDMENT PRIVILEGE-SEARCH AND SEIZURE ISSUES (2003) **HN: 5,8 (F.3d)**

16 68 Am. Jur. 2d Searches and Seizures s 330, -COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT (2003)

17 CALEA AND THE RIPA: THE U.S. AND THE U.K. RESPONSES TO WIRETAPPING IN AN INCREASINGLY WIRELESS WORLD, 12 Alb. L.J. Sci. & Tech. 125, 166+ (2001) **HN: 5,8,9 (F.3d)**

18 CALEA AND THE RIPA: THE U.S. AND THE U.K. RESPONSES TO WIRETAPPING IN AN INCREASINGLY WIRELESS WORLD, 12 Alb. L.J. Sci. & Tech. 125, 166+ (2001) **HN: 5,8,9 (F.3d)**

19 WATCH WHAT YOU TYPE: AS THE FBI RECORDS YOUR KEYSTROKES, THE FOURTH AMENDMENT DEVELOPS CARPAL TUNNEL SYNDROME, 40 Am. Crim. L. Rev. 1271, 1300+ (2003) **HN: 5,8,9 (F.3d)**

20 1 Andrews Electronic Privacy Litigation Reports 4, D.C. CIRCUIT VACATES PART OF CALEA ORDER U.S. Telecom Ass'n v. FCC (2000) **HN: 8 (F.3d)**

21 4 Andrews Telecomm. Industry Litig. Rep. 6, D.C. CIR. VACATES PART OF CALEA ORDER U.S. Telecom Ass'n v. FCC (2000)

22 REGULATION ON THE HORIZON: ARE REGULATORS POISED TO ADDRESS THE STATUS OF IP TELEPHONY?, 11 CommLaw Conspectus 19, 44 (2003)

23 CARNIVORE: THE UNEASY RELATIONSHIP BETWEEN THE FOURTH AMENDMENT AND ELECTRONIC SURVEILLANCE OF INTERNET COMMUNICATIONS, 9 CommLaw Conspectus 111, 129+ (2001) **HN: 5,8,10 (F.3d)**

24 FIRE WITH FIRE: HOW THE FBI SET TECHNICAL STANDARDS FOR THE TELECOMMUNICATIONS INDUSTRY UNDER CALEA, 8 CommLaw Conspectus 329, 348+ (2000) **HN: 6,10 (F.3d)**

25 BEYOND PRIVACY: CONFRONTING LOCATIONAL SURVEILLANCE IN WIRELESS COMMUNICATION, 8 Comm. L. & Pol'y 1, 23 (2003) **HN: 9 (F.3d)**

26 PRIVACY AND MOBILE TELECOMMUNICATIONS, 19-SUM Comm. Law. 20, 23+ (2001) **HN: 9 (F.3d)**

27 PRIVACY AND LAW ENFORCEMENT IN THE DIGITAL AGE, 18-WTR Comm. Law. 3, 3+ (2001) **HN: 5,8,10 (F.3d)**

28 MAKING AND KEEPING REGULATORY PROMISES, 55 Fed. Comm. L.J. 1, 60 (2002)

29 TOO MUCH POWER, TOO LITTLE RESTRAINT: HOW THE FCC EXPANDS ITS REACH THROUGH UNENFORCEABLE AND UNWIELDY "VOLUNTARY" AGREEMENTS, 53 Fed. Comm. L.J. 49, 68+ (2000) **HN: 5 (F.3d)**

30 WHAT BIG EYES AND EARS YOU HAVE!: A NEW REGIME FOR COVERT GOVERNMENTAL SURVEILLANCE, 70 Fordham L. Rev. 1017, 1109+ (2001) **HN: 5,8,9 (F.3d)**

31 PRIVACY VERSUS PROTECTION: EXPLORING THE BOUNDARIES OF ELECTRONIC SURVEILLANCE IN THE INTERNET AGE, 29 Fordham Urb. L.J. 2233, 2276+ (2002) **HN: 5,6,10 (F.3d)**

32 PURVEYORS OF HATE ON THE INTERNET: ARE WE READY FOR HATE SPAM?, 17 Ga. St. U. L. Rev. 379, 407 (2000) **HN: 10 (F.3d)**

33 THE CASE AGAINST CARNIVORE: PREVENTING LAW ENFORCEMENT FROM DEVOURING PRIVACY, 35 Ind. L. Rev. 303, 328+ (2001) **HN: 5 (F.3d)**

34 AN FCC NEMESIS, 3/19/01 Nat'l L.J. B1, col. 1, B1, col. 1+ (2001) **HN: 8 (F.3d)**

35 WILL CARNIVORE DEVOUR THE FOURTH? AN EXPLORATION OF THE CONSTITUTIONALITY OF THE FBI CREATED SOFTWARE, 18 N.Y.L. Sch. J. Hum. Rts. 305, 335+ (2002) **HN: 8,9,10 (F.3d)**

36 STATUTES-TELECOMMUNICATIONS-FROM CALEA TO CARNIVORE: HOW UNCLE SAM CONSCRIPTED PRIVATE INDUSTRY IN ORDER TO WIRETAP DIGITAL TELECOMMUNICATIONS U.S. Telecom Ass'n v. FCC, 227 F.3d 450 (D.C. Cir. 2000), 77 N.D. L. Rev. 795, 801+ (2001) **HN: 5,8,10 (F.3d)**

Citing References

Secondary Sources (U.S.A.)

37 INTERNET SURVEILLANCE LAW AFTER THE USA PATRIOT ACT: THE BIG BROTHER THAT ISN'T, 97 Nw. U. L. Rev. 607, 673+ (2003) **HN: 8 (F.3d)**

38 UNRESTRICTED FEDERAL AGENT: "CARNIVORE" AND THE NEED TO REVISE THE PEN REGISTER STATUTE, 76 Notre Dame L. Rev. 1215, 1259+ (2001) **HN: 2,8,9 (F.3d)**

39 FBI INTERNET SURVEILLANCE: THE NEED FOR A NATURAL RIGHTS APPLICATION OF THE FOURTH AMENDMENT TO INSURE INTERNET PRIVACY, 8 Rich. J.L. & Tech. 1, 16+ (2002) **HN: 5,8,10 (F.3d)**

40 THE SOFTWARE FORMERLY KNOWN AS "CARNIVORE": WHEN DOES E-MAIL SURVEILLANCE ENCROACH UPON A REASONABLE EXPECTATION OF PRIVACY?, 52 S.C. L. Rev. 875, 894+ (2001) **HN: 8 (F.3d)**

41 DIGITAL DOSSIERS AND THE DISSIPATION OF FOURTH AMENDMENT PRIVACY, 75 S. Cal. L. Rev. 1083, 1167 (2002) **HN: 10 (F.3d)**

42 ADMINISTRATIVE WAIVER OF THE UNTIMELINESS DEFENSE IN TITLE VII CASES CONCERNING FEDERAL EMPLOYEES: A PROPOSED ANALYSIS, 46 St. Louis U. L.J. 477, 507 (2002)

43 FAIR INFORMATION PRACTICES AND THE ARCHITECTURE OF PRIVACY (WHAT LARRY DOESN'T GET), 2001 Stan. Tech. L. Rev. 1, 121 (2001)

44 BIG BROTHER WHERE ART THOU, ELECTRONIC SURVEILLANCE AND THE INTERNET: CARVING A WAY FOURTH AMENDMENT PRIVACY PROTECTIONS, 32 Tex. Tech L. Rev. 1053, 1075+ (2001) **HN: 5,9,10 (F.3d)**

45 COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT (CALEA), 36-APR Prosecutor 22, 32 (2002) **HN: 5 (F.3d)**

46 ESTABLISHING A RATIONAL BASIS FOR REGULATING ANIMAL FEEDING OPERATIONS: A VIEW OF THE EVIDENCE, 27 Vt. L. Rev. 115, 147+ (2002) **HN: 4,7 (F.3d)**

47 ISSUES RAISED BY THE APPLICATION OF THE PEN REGISTER STATUTES TO AUTHORIZE GOVERNMENT COLLECTION OF INFORMATION ON PACKET-SWITCHED NETWORKS, 6 Va. J.L. & Tech. 4, 22+ (2001) **HN: 5,8,10 (F.3d)**

48 CARNIVORES, CYBER SPIES & THE LAW, 74-FEB Wis. Law. 14, 15+ (2001) **HN: 8 (F.3d)**

49 INTERNATIONAL HUMAN RIGHTS LAW CHALLENGES TO THE NEW INTERNATIONAL CRIMINAL COURT: THE SEARCH AND SEIZURE RIGHT TO PRIVACY, 26 Yale J. Int'l L. 323, 412 (2001) **HN: 8 (F.3d)**

50 116 BNA Daily Report for Executives A-1, 2002, PRIVACY: DEADLINE LOOMS AS FCC REAFFIRMS ELECTRONIC SURVEILLANCE CAPABILITIES (2002) **HN: 5 (F.3d)**

51 , 731 PLI/Pat 87, 126+ (2002) **HN: 2,5,8 (F.3d)**

52 RECENT DEVELOPMENTS IN U.S. PRIVACY LAW, INCLUDING POST-SEPTEMBER 11, 2001, 701 PLI/Pat 11, 43 (2002) **HN: 6 (F.3d)**

53 RECENT DEVELOPMENTS IN U.S. PRIVACY LAW, 681 PLI/Pat 7, 34 (2001) **HN: 6 (F.3d)**

Briefs (U.S.A.)

54 U.S., People v. F.E.R.C., 2001 WL 396519 (Apr 19, 2001) ** **HN: 4 (F.3d)**

itation
7 FR 21999-01
002 WL 820189 (F.R.)
Cite as: 67 FR 21999)

KeyCite Citing

Rank 1 of 1

Database
FR

RULES and REGULATIONS

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Parts 22, 24 and 64

[CC Docket No. 97-213; FCC 02-108]

Communications Assistance for Law Enforcement Act

Thursday, May 2, 2002

21999 AGENCY: Federal Communications Commission.

CTION: Final rule.

UMMARY: This document adopts four electronic surveillance capabilities for ireline, cellular, and broadband Personal Communications Services ("PCS") elecommunications carriers and sets a compliance date of June 30, 2002 for those our capabilities, as well as two capabilities previously mandated by the ommission. The Commission takes this action under the provisions of the ommunications Assistance for Law Enforcement Act of 1994 (Public Law 103- 414, 08 Stat. 4279 (1994) (codified as amended in scattered sections of 18 U.S.C. and 7 U.S.C. 229, 1001-1010, 1021)). ("CALEA") and in response to a decision issued y the United States Court of Appeals for the District of Columbia Circuit "Court") that vacated four Department of Justice ("DoJ")/Federal Bureau of nvestigation ("FBI") "punch list" electronic surveillance capabilities mandated y the Commission's Third Report and Order ("Third R&O") in this proceeding.

ATES: Effective June 3, 2002.

OR FURTHER INFORMATION CONTACT: Jamison Prime, Office of Engineering and echnology, (202) 418-7474, TTY (202) 418-2989, e-mail: jprime@fcc.gov or Rodney mall, Office of Engineering and Technology, (202) 418-2452, TTY (202) 418-2989, -mail rsmall@fcc.gov.

UPPLEMENTARY INFORMATION: This is a summary of the Commission's Order on Remand, C Docket No. 97-213, FCC 02-108, adopted April 5, 2002, and released April 11, 002. The full text of this document is available on the Commission's internet ite at www.fcc.gov. It is also available for inspection and copying during egular business hours in the FCC Reference Center (Room CY- A257), 445 12th treet., SW, Washington, DC 20554. The complete text of this document may be urchased from the Commission's duplication contractor, Qualex International, 202) 863-2893 voice, (202) 863-2898 Fax, qualexint@aol.com e- mail, Portals II, 45 12th St., SW, Room CY-B402, Washington, DC 20554.

2

ummary of Order on Remand

1. The Order on Remand adopts additional technical requirements for wireline, ellular, and broadband PCS carriers to comply with the assistance capability equirements prescribed by CALEA and sets a June 30, 2002 compliance date for arriers to provide these capabilities. Section 103(a) of CALEA requires that a elecommunications carrier shall ensure that its equipment, facilities, or ervices that provide a customer or subscriber with the ability to originate, erminate, or direct communications are capable of isolating and providing to the overnment, pursuant to a lawful authorization, certain wire and electronic ommunications, including call-identifying information that is reasonably vailable to the carrier. Under section 107(a)(2) of CALEA (the "safe harbor" rovision), carriers and manufacturers that comply with industry standards for lectronic surveillance are deemed in compliance with their specific esponsibilities under CALEA, but, if industry associations or standard-setting rganizations fail to issue technical requirements or standards or if a overnment agency or any other person believes that such requirements or tandards are deficient, the Commission is authorized in response to a petition rom any Government agency or person, to establish, by rule, technical equirements or standards. Under section 107 (b) of (CALEA) technical equirements or standards adopted by the Commission must meet the assistance apability requirements of section 103 by cost-effective methods; protect the rivacy and security of communications not authorized to be intercepted; minimize he cost of such compliance on residential ratepayers; serve the policy of the nited States to encourage the provision of new technologies and services to the ublic; and provide a reasonable time and conditions for compliance with and the ransition to any new standard.

2. In the Third R&O, 14 FCC Rcd 16794, 64 FR 51710, September 24, 1999, the ommission required that ***22000** wireline, cellular, and broadband PCS carriers mplement all electronic surveillance capabilities of the industry interim tandard, J-STD-025 ("J-Standard") and six of nine additional capabilities equested by DoJ/FBI, known as the "punch list" capabilities. With respect to the ix required punch list capabilities, "dialed digit extraction" would provide to aw enforcement agencies ("LEAs") those digits dialed by a subject after the nitial call setup is completed; "party hold/join/drop" would provide to LEAs nformation to identify the active parties to a conference call; "subject-nitiated dialing and signaling" would provide to LEAs access to all dialing and ignaling information available from the subject, such as the use of flash-hook nd other feature keys; "in-band and out-of-band signaling" would provide to LEAs nformation about tones or other network signals and messages that a subject's ervice sends to the subject or associate, such as notification that a line is inging or busy; "subject- initiated conference calls" would provide to LEAs the ontent of conference calls supported by the subject's service; and "timing nformation" would provide to LEAs information necessary to correlate call-dentifying information with call content.

3. Several parties challenged the Commission's decision before the Court. In ts August 15, 2000 Remand Decision, 227 F. 3d 450, the Court affirmed the ommission's findings in the Third R&O in part and vacated and remanded for

urther proceedings the Third R&O's decisions concerning four punch list apabilities (dialed digit extraction, party hold/join/drop messages, subject-nitiated dialing and signaling information, and in-band and out-of-band ignaling information).

4. Section 102(2) of CALEA defines "call-identifying information" as "dialing r signaling information that identifies the origin, direction, destination, or ermination of each communication generated or received by a subscriber by means f any equipment, facility, or service of a telecommunications carrier." The J-tandard further interprets the key terms in this definition as follows: origin s the number of the party initiating the call (e.g., calling party); termination s the number of the party ultimately receiving a call (e.g., answering party); irection is the number to which a call is re-directed or the number from which t came, either incoming or outgoing (e.g., redirected-to party or redirected-rom party); and destination is the number of the party to which a call in being ade (e.g., called party). Although the J-Standard adopts definitions that frame all-identifying information in terms of telephone numbers, the Commission, in he Third R&O, found capabilities required under CALEA, in some cases, require arriers to disclose information that is not a telephone number. The Court held hat CALEA is ambiguous as to precisely what constitutes call-identifying nformation and thus, what the CALEA requirements are. In cases where the intent f Congress is not clear, an agency may develop its interpretation of the statute ithin the guidelines set forth in Chevron v. National Resources Defense Counsel, nc., 467 U.S. 837 (1984), and subsequent cases.

5. The J-Standard's definitions do not give all portions of CALEA full effect, nd we are disinclined to interpret a statute in a manner that will render ortions of it superfluous. The legislative history of CALEA does not clearly tate Congress's intent with respect to the key terms at issue, and we think it ould be implausible to read CALEA as providing for a more limited class of nformation than that which LEAs already receive. Nor do we find a basis for ying our interpretation of CALEA exclusively to a prior, separate statute, such s the Electronic Communications Privacy Act of 1986 ("ECPA"). In the Remand ecision, the Court stated that CALEA does not cross-reference or incorporate the efinitions of pen registers and trap and trace devices in the ECPA. Moreover, he standards have been modified by such legislation as the USA PATRIOT Act, hich expands the terms "pen register" and "trap and trace device" to include the oncept of "dialing, routing, addressing, or signaling information."

6. We are adopting a definition of "call-identifying information" that eplicates the existing electronic surveillance capability functions, but that is lso expressed in sufficiently broad terms so as not to be limited to a specific etwork technology. This analysis is consistent with overall purpose expressed or the Act: CALEA was intended to preserve the ability of law enforcement fficials to conduct electronic surveillance effectively and efficiently in the ace of rapid advances in telecommunications technology. An example of this pproach can be found in the Court's upholding of the provision of antenna ocation information, even though this capability has no structural equivalent in he traditional wireline architecture. Similarly, we note that there are many ituations in which a party inputs dialing information that, in itself, is not a elephone number.

7. Although "call-identifying information" consists of both dialing and ignaling information that may or may not be described in terms of telephone umbers, not all dialing and signaling information is "call-identifying nformation." While some dialing or signaling information identifies the origin, irection, destination, or termination of a communication, other dialing or ignaling information--such as a bank account number in a bank-by- phone system--learly does not. Insofar as a ringing tone or a busy signal provides nformation that is descriptive of an origin, direction, destination, or ermination a communication, that tone or signal "identifies" such a ommunication for purposes of CALEA and falls within CALEA's definition of "call-dentifying information." By contrast, call content does not identify the origin, ermination, direction, and destination of a communication, and thus is not "call dentifying information" for purposes of CALEA. Section 102(2) of CALEA defines all-identifying information as "dialing or signaling information that identifies he origin, direction, destination, or termination" of each call or ommunication. Thus, the origin, direction, destination, or termination is dentified by call-identifying information, such as the caller's phone number. he J-Standard's definitions are deficient to the extent that they claim that a hone number is itself an origin, direction, destination, and termination.

8. In a simple two-way telephone call, the dialing or signaling information hat identifies the "origin" of a communication is the calling party's telephone ine (which is commonly identified by a telephone number). There are situations n which information other than a number is needed to identify the party nitiating a call. For example, when a wireless phone is used to initiate a all, that origin may be identified by both the number assigned to the wireless hone and the location information of the antenna site to which the phone is onnected. Because the origin pertains to a calling party, there may be multiple oints in a telephone call scenario that give rise to information that identifies he origin of a communication.

9. We conclude that a "termination" is a party or place at the end of a ommunication path. The J-Standard defines "termination" in terms of the "party ltimately receiving the call." Common practice as well as the industry's own echnical standards suggest a broader definition that recognizes that a call can terminate" ***22001** when it reaches an identifiable stopping point in the etwork. The J-Standard shows a diagram where the surveillance subject ("S") is onnected to one party ("A"), while the other party ("B") is on hold. As shown n the diagram, the communication path starting from party A terminates at S. owever, as is also shown in the diagram, the communication path coming from the eld party B terminates at the subject's switch, and not at the subject's line. his example also supports the proposition that a termination is not always dentified by a telephone number because (1) a network switch is not a party in a all, and (2) a network switch is a point in the network with no directory elephone number. There can be multiple terminations within a single call ecause there are multiple points in a call at which there is information that dentifies the called party.

10. A "destination" is a party or place to which a call is being made. We reach his definition after considering common and technical dictionary definitions of he term, as well as that provided by the J-Standard. Similarly, we agree with

he J-Standard's general characterization of "direction" as a description of avigation within a network but reject the contention that this information is xclusively a telephone number. We find that the "direction" is, broadly peaking, information that identifies the path of communication.

11. Thus, we are defining the relevant terms as follows: origin is a party nitiating a call (e.g., a calling party), or a place from which a call is nitiated; destination is a party or place to which a call is being made (e.g., he called party); direction is a party or place to which a call is re-directed r the party or place from which it came, either incoming or outgoing (e.g., a edirected-to party or redirected-from party); and termination is a party or lace at the end of a communication path (e.g., the called or call-receiving arty, or the switch of a party that has placed another party on hold). These hanges distinguish between origin, destination, direction, and termination, and he information that identifies them; permit multiple origins, destinations, irections, and terminations in a call; and provide for terminations inside a etwork switch or at another point within a network. Moreover, this approach efines call-identifying information in a manner that can be converted into ctual network capabilities, unlike the definition suggested by DoJ/FBI.

12. Under sections 107(b)(1) and 107(b)(3) of CALEA, if the Commission finds hat industry-established technical standards are deficient, it may establish tandards that "meet the assistance capability requirements of section 103 by ost-effective methods" and "minimize the cost of such compliance on residential atepayers." The Court was unable to find a rational connection between the facts ound and the choice made in the Third R&O. CALEA does not define "cost-ffective." One approach for determining whether something is "cost-effective" hat is consistent with the Court's analysis in its Remand Decision is to compare wo or more ways of accomplishing a task and identifying the process that is the east expensive. This approach is supported by the Commission's own rules, other tatutes where Congress has defined or described the term, as well as in other gencies' rules. Thus, it makes sense to consider whether a particular option is etter than some alternative at achieving some particular regulatory requirement, hen such a comparison is available. We first inquire whether we have in the ecord an alternative means to accomplish each of the punch list capabilities.

13. When a punch list capability "meet(s) the assistance capability equirements" of CALEA, but there is no alternative means of accomplishing the ame task, we will then consider whether the capability serves to minimize costs. n general, something is "effective" if it accomplishes a task in an efficient anner. However, we will not adopt or reject a capability solely on the basis of cost-benefit analysis because Congress has already made such a calculation when t determined the assistance capability requirements of CALEA. There are costs ssociated with CALEA, and it is clear that Congress anticipated that carriers ould bear some of these costs. However, as part of our examination of whether a echnical standard that we require under CALEA is "cost-effective," we will onsider the financial burden it places on carriers. In the case of the punch ist capabilities, we note that several aspects of the implementation program ignificantly mitigate this burden, which serves to make implementation of the unch list capabilities "cost-effective" for carriers. These features include oJ/FBI cost reimbursement programs, buyout agreements with manufacturers to pay

or all necessary software upgrades, and deferral of required punch list apabilities coincident with routine switch upgrades. Also, five elecommunications equipment manufacturers have incorporated all six punch list apabilities required by the Third R&O into one software upgrade, and it is nclear whether deleting one or more of these capabilities from that upgrade will essen the cost of the upgrade to those carriers that purchase software from anufacturers that are not covered by the DoJ/FBI buyout agreements. Carriers ay also recover at least a portion of their CALEA software and hardware costs by harging to LEAs, for each electronic surveillance order authorized by CALEA.

14. In considering the effect of CALEA compliance on residential ratepayers nder section 107(b)(3) we look at the effect on residential wireline subscribers nly. Although CALEA does not define the term "residential ratepayers," floor ebate emphasized concern over "basic residential telephone service" rates. ireless telecommunications services such as cellular or PCS are intrinsically obile services, and we have not previously attempted to describe what "basic esidential" service is in the wireless context, nor have we differentiated etween residential and other classes of wireless service. By contrast, the oncept of "residential ratepayer" has historically been used in the context of ate regulation for wireline telecommunication service, which traditionally ifferentiates rates for residential and business customers. Other provisions of ALEA can only apply to wireline telecommunications carriers, as states do not ave authority to regulate rates for commercial mobile radio services and the ommission has forborne from such rate regulation under legislation and ommission decisions that were adopted prior to CALEA.

15. The general approach we have taken with our analysis of "cost-effective" is pplicable in considering ways of minimizing the impact on residential atepayers. That which is "cost-effective" is also likely to correlate to the ffect on residential ratepayers, and so many of the factors we have previously dentified will apply in this context. We conclude that the capabilities that we ave identified--and the means of implementing them--do serve to minimize the ost on residential ratepayers. To the extent that there are costs borne by the arriers and passed through to customers, we note that it is likely that the osts would be shared by all ratepayers and, therefore, would be significantly iluted on an individual residential ratepayer basis. The fact that costs are pread across such a large base in itself suggests another means by which rovision of these capabilities will minimize the effect on residential atepayers--that the cost of CALEA compliance for any ***22002** particular esidential ratepayer will be minimal.

16. We note, however, that, even if the definition of "residential taxpayers" is roadened to include households that use wireless telephone service as a ubstitute for local wireline telephone service, there is no reason to believe hat implementation of the punch list items would fail to minimize the cost on ireless residential ratepayers. In the Third R&O, the Commission found that ive major telecommunications manufacturers--which account for the great majority f sales to wireline, cellular, and broadband PCS carriers in the United States--nticipated total revenues from carriers purchasing the four vacated punch list apabilities of about $277 million. Of this amount, about $159 million was nticipated in wireless revenues and about $117 million was anticipated in

ireline revenues. While these figures do not include all carrier costs of mplementing the four capabilities, in the Third R&O, we found that, relative to ther cost/revenue estimates, the manufacturers' estimates were "the most etailed and reliable." Further the FBI's buyout and flexible deployment rograms, coupled with manufacturers incorporating all punch list capabilities nto one software upgrade would likely lessen costs to such an extent that total osts of implementing the four vacated capabilities nationwide would be well elow $159 million to wireless carriers and $117 million to wireline carriers. onetheless, assuming pessimistically that those costs would eventuate and that hey would be passed on to wireless subscribers and residential wireline atepayers in full as a one-time charge, the respective charge per wireless ubscriber and residential wireline ratepayer would average about $1.45 and 1.20. Alternatively, if these costs to wireless and wireline carriers were onverted to a rate increase to wireless subscribers and residential wireline atepayers, the rate increase would average only pennies per month per ubscriber/ratepayer. Accordingly, we find that the likely worst case cost mpact of carriers implementing the four vacated capabilities would be minimal on oth wireless subscribers and residential wireline taxpayers.

17. The dialed digit extraction capability would require the telecommunications arrier to provide to the LEA on the call data channel the identity of any digits ialed by the subject after connecting to another carrier's service (also known s "post-cut-through digits"). The dialed digit extraction capability provides all-identifying information. Post-cut-through digits identify, under many ircumstances, a communication's destination or a termination. For example, a arty may dial a toll-free number to connect to a long distance carrier (e.g. -800-CALL-ATT) and subsequently enter another phone number to be connected to a arty. That second number identifies a "destination" because it is "a party or lace to which a call is being made." If a successful connection is made, that econd number also identifies a "termination" because it is the called or call- eceiving party. A subject may also dial digits that are not call-identifying nformation--such as a bank account or social security number. However, many ost-cut-through dialed digits simply route the call to the intended party and re, therefore, unquestionably call-identifying information even under a narrow nterpretation of that term.

18. Section 103(a) of CALEA requires carriers to be capable of "expeditiously solating" wire and electronic communications and call-identifying information to nable LEAs to obtain this information "concurrently with their transmission from he subscriber's equipment, facility, or service. * * *" (in the case of the nterception of wire and electronic communications) or "before, during, or mmediately after the transmission of a wire or electronic communication" (in the ase of call-identifying information). Because of this timing requirement, we re rejecting the alternative of having a LEA serve the terminating carrier with pen register order to obtain those dialed digits that were placed once a call as been cut-through from the originating carrier. Under such a process, the overnment would be unable to obtain call-identifying information concurrently ith its transmission to or from a subscriber.

19. Dialed digit extraction is a capability that is "reasonably available to the arrier" under section 103 of CALEA. The J-Standard defines "reasonably

vailable" as information "present at an Intercept Access Point for call rocessing purposes." We reject the limitation that the information must be resent "for call processing purposes" for it to be "available." We read reasonably" as a qualifier; if information is only accessible by significantly odifying a network, then we do not think it is "reasonably" available.
20. Section 107(b)(2) requires that any standards we require must "protect the rivacy and security of communications not authorized to be intercepted." There urrently appears to be no technology that can separate those post-cut-through ialed digits from other post-cut-through dialed digits that are not call- dentifying (i.e., that are call content). Because post-cut-through digits nclude call-identifying information, LEAs should be able to obtain this nformation under CALEA so long as they have a valid legal instrument. Although a itle III warrant--which would give a LEA call content--may be one such valid nstrument, it is not up to us to decide whether it is the only one that could be sed. Were we to conclude that a Title III warrant represents an alternative eans of accomplishing the dialed digit extraction capability we would ecessarily have to assume that a pen register does not entitle a LEA to dialed igit extraction. Such a decision would improperly usurp the role of the courts o decide what legal instrument is necessary to obtain the dialed digit nformation. Our approach is similar to the approach that we employed with espect to a packet-mode communications capability, which was upheld by the Court n the Remand Decision.
21. Because the standards we adopt must protect the privacy and security of ommunications not authorized to be intercepted, we reject the proposal to allow LEA to extract dialed digits on content channels using their own decoders. his alternative is not acceptable because it would require the LEA in every ase, no matter the level of authorization involved, to obtain the entire content hen a less intrusive alternative (dialed digit extraction, whereby carriers eparate out tone information) is available. This alternative would also shift rom carriers to LEAs responsibility for ensuring that interceptions are onducted in a way that protects the privacy and security of communications not uthorized for interception as much as possible. Such a result would be nconsistent with section 103(a)(4) of CALEA, which requires carriers to protect he privacy and security of communications and call- identifying information not uthorized to be intercepted.
22. In order to respond to the appropriate legal authority, a carrier must have he ability to turn on and off the dialed digit extraction capability. We elieve that a toggle feature for dialed digit extraction is necessary in order o protect privacy interests under certain circumstances, without disrupting the arrier's ability to provide other punch list capabilities included in the same oftware. We therefore conclude that carriers must have the equipment and oftware to ***22003** support a dialed digit extraction capability with a toggle eature. Where such a toggle feature will not be available from a carrier's endor by the compliance deadline, that carrier may file a petition with the ommission under section 107(c), requesting an extension of the compliance eadline.
23. The party hold/join/drop messages capability would permit the LEA to receive rom the telecommunications carrier messages identifying the parties to a

onference call at all times. The party hold message would be provided whenever ne or more parties are placed on hold. The party join message would report the ddition of a party to an active call or the reactivation of a held call. The arty drop message would report when any party to a call is released or isconnects and the call continues with two or more other parties. Under our evised definitions of the components of call-identifying information, party old/join/drop information is call-identifying information because it identifies hanges in the origin(s) and termination(s) of each communication generated or eceived by the subject. Further, by isolating call-identifying information in his manner, the LEA may more readily avoid monitoring the communications of hird parties who are not privy to the communications involving the subject, hereby furthering privacy considerations. In the Third R&O, the Commission efined call-identifying information to be "reasonably available" to an riginating carrier if such information "is present at an [Intercept Access oint] and can be made available without the carrier being unduly burdened with etwork modifications." The J-Standard acknowledges that the network must ecognize and process party hold/join/drop functions as part of its basic peration. Thus, we conclude that party hold/join/drop information is not only resent at an Intercept Access Point but, because it is already being used by the arrier, satisfies the definition of "reasonably available" in the original ersion of the J-Standard.

24. The subject-initiated dialing and signaling information capability would ermit the LEA to be informed when a subject sends signals or digits to the etwork. This capability would require the telecommunications carrier to deliver message to the LEA, for each communication initiated by the subject, informing he LEA whenever the subject has invoked a feature during a call, including eatures that would place a party on hold, transfer a call, forward a call, or dd/remove a party to a call. This capability constitutes call- identifying nformation because it provides information regarding the party or place to which forwarded call is redirected and because it provides information regarding a aiting calling party. Signals such as on-hook, off- hook, and flash-hook ignals, which are generated by a subject, are reasonably available to the arrier because they must be processed at the carrier's Intercept Access Point. TMF signals generated by a subject that must be processed at the Intercept ccess Point also are reasonably available to the carrier; however, some DTMF ignals generated by the subject are post-cut- through digits, and those signals re covered under dialed digit extraction.

25. The in-band and out-of-band signaling information capability would enable a elecommunications carrier to send a notification message to the LEA when any all-identifying network signal (e.g., audible ringing tone, busy, call waiting ignal, message light trigger) is sent to a subject. For example, if someone eaves a voice mail message on the subject's phone, the notification to the LEA ould indicate the type of call-identifying network signal sent to the subject e.g., stutter dial tone, message light trigger). For calls the subject riginates, a notification message would also indicate whether the subject ended call when the line was ringing, busy (a busy line or busy trunk), or before the etwork could complete the call. Authorizing this capability for call- dentifying information that is based on network signals that originate on

arriers' own networks conforms with CALEA. While certain types of signals used y carriers for supervision or control do not trigger any audible or visual essage to the subscriber and are therefore not call-identifying information, ther types of signals--such as ringing and busy tones--are call- identifying nformation under our revised definitions because they convey information about he termination of a call. For example, when a subject calls another party, ntil the called party answers the subject's communications path is terminated at n audible ringing tone generator. However, if the called party is engaged in nother conversation and does not have call waiting, the subject's communications ath is terminated at a busy signal generator. Thus, even for calls from the ubject that are never answered, the fact that the subject hears busy or audible inging signal provides call-identifying information that is not provided to law nforcement via other means. The J- Standard is inadequate in this regard. For xample, the fact that a call attempt does not result in a conversation because he line is busy or because the called party does not answer does not mean that o "communication" has taken place. In-band and out-of-band signals that are enerated at the carrier's Intercept Access Point toward the subscriber are andled by the carrier and are clearly available to the carrier at an Intercept ccess Point, and convey call-identifying information. Because carriers already eliver this information to subscribers, we see no reason why it cannot also be ade available to LEAs without significantly modifying the carrier's network. hus, in-band and out-of-band signaling information is "reasonably available."

26. For each of the punch list items, Commenters have presented no alternative ays of obtaining all the information encompassed by this capability or those lternatives (in the case of dialed digit extraction) have deficiencies that make hem unsatisfactory. Because there are no alternative means of accomplishing hese objectives, we cannot engage in a cost-comparison analysis. Mechanisms uch as the FBI's buyout and flexible deployment programs, coupled with five anufacturers incorporating all punch list capabilities into one software pgrade, will lessen software costs significantly, and including or not including ny one of these capabilities may not significantly change carriers' costs. ecause of these cost-mitigation measures, we find that it will be cost-effective o require these capabilities. For similar reasons, the capabilities are nlikely to significantly affect residential ratepayers. The aforementioned rograms will serve to mitigate carriers' costs, which in turn will reduce the osts that carriers may pass on to ratepayers. Moreover, carriers will also be ble to spread costs across a large ratepayer base and there is no indication hat the compliance costs will be disproportionately borne by residential atepayers. Although we have addressed privacy issues with respect to dialed igit extraction, we see no significant privacy issues arising from grant to LEAs f the remaining capabilities. No party to this proceeding challenged the Third &O's decision with respect to those capabilities on privacy grounds, and the ourt did not cite privacy as a basis for remanding to the Commission the Third &O's decision with respect to that capability.

27. Section 107(b)(4) of CALEA--i.e., serve the policy of the United States to ncourage the provision of new technologies and services to the public--was not riefed to or addressed by the Court in its Remand Decision. As ***22004** described n the legislative history, one of the key concerns in enacting CALEA was "the

oal of ensuring that the telecommunications industry was not hindered in the apid development and deployment of the new services and technologies that ontinue to benefit and revolutionize society." Aside from one suggestion that he cost of compliance would divert capital from new technology deployment, no ommenter has argued--nor is there anything in the record to suggest--that nclusion of the four punch list requirements would impede in any way the rovision of new telecommunications technologies or services to the public or ould delay in any manner the course or current pace of technology. Rather, the unch list requirements represent a technical solution that interfaces with the arriers' own network designs to provide LEAs with interception access and the apability to intercept wire and electronic communications. Additionally, as oted above, for the majority of switches, carriers will be permitted under the BI's flexible deployment program to implement any required punch list apabilities coincident with routine switch upgrades. Moreover, we do not elieve section 107(b)(4) was intended to bar a feature simply because it imposes osts on telecommunications companies and thereby might affect their other pending. The two express references to costs in section 107(b) (i.e., cost ffectiveness and minimizing impact on residential ratepayers) consider cost in a elative, not an absolute, sense. Accordingly, we do not believe paragraph (b)(4) as intended to prohibit any feature because the cost might have some impact on elecommunications companies' other spending. Given this, we find that adoption f the punch list requirements is consistent with the United States' policy of ncouraging the provision of new technologies and services to the public.

28. Section 107(b)(5) of CALEA requires that the Commission "provide a easonable time and conditions for compliance with and the transition to any new tandard, including defining the obligations of telecommunications carriers under ection 103 during any transition period." The Third R&O required that the six unch list capabilities be implemented by wireline, cellular, and broadband PCS arriers by September 30, 2001 and five telecommunications switch manufacturers ave incorporated all of these capabilities into one software upgrade. In the rder in this proceeding, which suspended the September 30, 2001 deadline for all unch list capabilities, including the two unchallenged capabilities (i.e., ubject-initiated conference calls and timing information), we indicated that we nticipated establishing June 30, 2002 as the new compliance date for all equired punch list capabilities as we expected to address the Court's Remand ecision by year's end and given that the record indicates that carriers can mplement any required changes to their software within six months of our ecision. We find it reasonable to require wireline, cellular, and broadband PCS arriers to implement all punch list capabilities by June 30, 2002, and conclude hat the June 30, 2002 deadline will satisfy section 107(b)(5). At the initial tages of CALEA implementation, the Commission found that carriers could put into ffect any required changes to their network within six months of its decision. e recognize that this is a more aggressive timetable than the six months we nticipated earlier. We believe that this accelerated compliance schedule is easonable for this stage of the CALEA implementation, as carriers have been ware of the CALEA capabilities under consideration in the instant Order on emand since October 2000. In addition, the record indicates that much of the oftware required to implement the punch list items has already been developed,

hich should significantly speed implementation. Finally, carriers have much reater experience in meeting CALEA's capability requirements than they had in 998. Together, these factors make a shorter implementation timetable reasonable. herefore, we are lifting the suspension of the punch list compliance deadline, nd specifying the revised punch list compliance deadline as June 30, 2002.
29. We note that carriers who are unable to comply may seek relief under the pplicable provisions of CALEA. The Wireline Competition Bureau (formerly, the ommon Carrier Bureau) and the Wireless Telecommunications Bureau previously ssued a Public Notice outlining the petitioning process for telecommunications arriers seeking relief under section 107(c) for an extension of the CALEA ompliance deadline. Carriers seeking relief from the June 30, 2002 compliance ate should follow the procedures outlined in that Public Notice. We further ote that, in most cases, extensions that the Commission has already granted will pply to the capabilities we are requiring in this Order on Remand. As the ireline Competition and Wireless Telecommunications Bureaus have previously tated: "Unless the Commission action [granting an extension] specifies therwise, the extension applies to all assistance capability functions, ncluding punch list and packet-mode capabilities, at the listed facilities."

upplemental Final Regulatory Flexibility Analysis

A) Need for and Purpose of This Action

30. As required by the Regulatory Flexibility Act (RFA), [FN1] the Commission ncorporated an Initial Regulatory Flexibility Analysis (IRFA) in the Further PRM. [FN2] The Commission sought written public comments on the proposals in the urther NPRM, including the IRFA. In the Third R&O, the Commission adopted a inal Regulatory Flexibility Analysis (FRFA). [FN3] As part of the instant Order n Remand, we have prepared this Supplemental FRFA to conform to the RFA. [FN4]

FN1 See 5 U.S.C. 603. The RFA, see 5 U.S.C. 601 et. seq., has been amended by he Contract With America Advancement Act of 1996, Pub. L. No. 104-121, 110 Stat. 47 (1996) (CWAAA). Title II of the CWAAA is the Small Business Regulatory nforcement Fairness Act of 1996 (SBREFA).

FN2 Communications Assistance for Law Enforcement Act, Further Notice of roposed Rulemaking, 13 FCC Rcd 22632, 22695-703 (1998).

FN3 Communications Assistance for Law Enforcement Act, Third Report and Order, C Docket No. 97-213, 14 FCC Rcd 16794, 16852-59 (1999).

FN4 See 5 U.S.C. 604.
31. The Third R&O responded to the legislative mandate contained in the ommunications Assistance for Law Enforcement Act, Public Law 103-414, 108 Stat. 279 (1994) (codified as amended in sections of 18 U.S.C. and 47 U.S.C.). The ommission, in compliance with 47 U.S.C. 229, promulgates rules in this Order on emand to ensure the prompt implementation of section 103 of CALEA. This action imply responds to an Order of the United States Court of Appeals for the

7 FR 21999-01
Cite as: 67 FR 21999, *22004)

istrict of Columbia Circuit (the "Court") and puts into effect rules we riginally evaluated as part of the FRFA in the Third R&O. Also, as noted, we ave already done a FRFA for the rules at issue in the Third R&O.

32. In enacting CALEA, Congress sought to balance three key policies with CALEA: (1) to preserve a narrowly focused capability for law enforcement agencies to arry out properly authorized intercepts; (2) to protect privacy in the face of ncreasingly powerful and personally revealing technologies; and (3) to avoid mpeding the development of new communications services and ***22005** echnologies." [FN5] The rules adopted in this Order on Remand implement ongress's goal to balance the three key policies enumerated above. The objective f the rules is to implement as quickly and effectively as possible the national elecommunications policy for wireline, cellular, and broadband PCS elecommunications carriers to support the lawful electronic surveillance needs f law enforcement agencies in a manner that is responsive to the Court's remand f the Third R&O.

FN5 H.R. Rep. No. 103-827, 103rd Cong., 2d Sess (1994) at 13.

B) Summary of the Issues Raised by Public Comments

33. In the Further NPRM, the Commission performed an IRFA and asked for comments hat specifically addressed issues raised in the IRFA. No parties filed comments irectly in response to the IRFA. Similarly, as part of the pleading cycle that ollowed the Court's remand of the Third R&O, no parties filed comments directly n response to the IRFA or the FRFA. In response to non-RFA comments filed in his docket, the Commission modified several of the proposals made in the Further FPRM. These modifications include changes to packet switching, conference call ontent, in-band and out-of-band signaling, and timing information, as first liscussed in the Third R&O.

34. The Commission's effort to update the record in response to the Court's emand Order resulted in additional non-RFA comments. The Rural Cellular ssociation (RCA) asserts that the costs of additional communications assistance apabilities would impose undue cost burdens on and jeopardize the efficient lanning and development of facilities by small and rural carriers. Similarly, he National Telephone Cooperative Association (NTCA) claims that any regulation hich requires carriers to deploy or upgrade facilities disproportionally affects mall and rural carriers.

C) Description and Estimate of the Number of Entities Affected

35. The RFA directs agencies to provide a description of and, where feasible, an stimate of the number of small entities that may be affected by the action aken. [FN6] The RFA generally defines the term "small entity" as having the same eaning as the terms "small business," "small organization," and "small overnmental jurisdiction." [FN7] In addition, the term "small business" has the ame meaning as the term "small business concern" under the Small Business Act. [FN8] A small business concern is one that: (1) Is independently owned and perated; (2) is not dominant in its field of operation; and (3) satisfies any

dditional criteria established by the Small Business Administration (SBA). [FN9] small organization is generally "any not-for-profit enterprise which is ndependently owned and operated and is not dominant in its field." [FN10] ationwide, as of 1992, there were approximately 275,801 small organizations. FN11] Finally, "small governmental jurisdiction" generally means "governments of ities, counties, towns, townships, villages, school districts, or special istricts, with a population of less than 50,000." [FN12] As of 1992, there were pproximately 85,006 such jurisdictions in the United States. [FN13] This number ncludes 38,978 counties, cities, and towns; of these, 37,566, or 96 percent, ave populations of fewer than 50,000. [FN14] The United States Bureau of the ensus (Census Bureau) estimates that this ratio is approximately accurate for ll governmental entities. Thus, of the 85,006 governmental entities, we stimate that 81,600 (91 percent) are small entities.

FN6 5 U.S.C. 603(b)(3).

FN7 Id., 601(6).

FN8 5 U.S.C. 601(3) (incorporating by reference the definition of "small usiness concern" in 15 U.S.C. 632). Pursuant to the RFA, the statutory efinition of a small business applies "unless an agency, after consultation with he Office of Advocacy of the Small Business Administration and after opportunity or public comment, establishes one or more definitions of such term which are ppropriate to the activities of the agency and publishes such definition(s) in he Federal Register." 5 U.S.C. 601(3).

FN9 Small Business Act, 15 U.S.C. 632.

FN10 5 U.S.C. 601(4).

FN11 1992 Economic Census, U.S. Bureau of the Census, Table 6 (special abulation of data under contract to Office of Advocacy of the U.S. Small usiness Administration).

FN12 5 U.S.C. 601(5).

FN13 U.S. Dept. of Commerce, Bureau of the Census, "1992 Census of overnments."

FN14 Id.

36. The most reliable source of information regarding the total numbers of ertain common carrier and related providers nationwide appears to be data the ommission publishes annually in its Telecommunications Provider Locator report, erived from filings made in connection with the Telecommunications Relay Service TRS). [FN15] According to data in the most recent report, there are 5,679 nterstate service providers. [FN16] These providers include, inter alia, local xchange carriers, wireline carriers and service providers, interexchange arriers, competitive access providers, operator service providers, pay telephone

perators, providers of telephone service, providers of telephone exchange ervice, and resellers.

FN15 FCC, Common Carrier Bureau, Industry Analysis Division, Telecommunications rovider Locator, Tables 1-2 (November 2001) (Provider Locator). This report is vailable on-line at: http:// www.fcc.gov/Bureaus/Common_Carrier/Reports/FCC-tate_ Link/Locator/locat01.pdf. See also 47 CFR 64.601 et seq.

FN16 Provider Locator at Table 1.

37. We have included small incumbent local exchange carriers (LECs) [FN17] in his present RFA analysis. As noted above, a "small business" under the RFA is ne that, inter alia, meets the pertinent small business size standard (e.g., a elephone communications business having 1,500 or fewer employees), and "is not ominant in its field of operation." [FN18] The SBA's Office of Advocacy contends hat, for RFA purposes, small incumbent LECs are not dominant in their field of peration because any such dominance is not "national" in scope. [FN19] We have herefore included small incumbent LECs in this RFA analysis, although we mphasize that this RFA action has no effect on FCC analyses and determinations n other, non-RFA contexts.

FN17 See 47 U.S.C 251(h) (defining "incumbent local exchange carrier").

FN18 15 U.S.C. 632.

FN19 Letter from Jere W. Glover, Chief Counsel for Advocacy, SBA, to William E. ennard, Chairman, FCC (May 27, 1999). The Small Business Act contains a efinition of "small business concern," which the RFA incorporates into its own efinition of "small business." See 15 U.S.C. 632(a) (Small Business Act); 5 .S.C. 601(3) (RFA). SBA regulations interpret "small business concern" to nclude the concept of dominance on a national basis. 13 CFR 121.102(b).

38. Total Number of Telecommunications Entities Affected. The Census Bureau eports that, at the end of 1992, there were 3,497 firms engaged in providing elephone services, as defined therein, for at least one year. [FN20] This number ontains a variety of different categories of entities, including local exchange arriers, interexchange carriers, competitive access providers, cellular arriers, mobile service carriers, operator service providers, pay telephone perators, PCS providers, covered SMR providers, and resellers. It seems certain hat some of those 3,497 telephone service firms may not qualify as small ntities or small incumbent LECs because they are not "independently owned and perated." [FN21] For example, a PCS provider that is affiliated with an ***22006** nterexchange carrier having more than 1,500 employees would not meet the efinition of a small business. It seems reasonable to conclude, therefore, that ewer than 3,497 telephone service firms are small entity telephone service firms r small incumbent LECs that may be affected by the actions taken in this Order n Remand.

FN20 United States Dept. of Commerce, Bureau of the Census, 1992 Census of ransportation, Communications, and Utilities: Establishment of Firm Size, at

'irm Size 1-123 (1995) ("1992 Census").

FN21 15 U.S.C. 632(a)(1).

39. Wireline Carriers and Service Providers. The SBA has developed a definition f small entities for wired telecommunications carriers. The Census Bureau eports that there were 2,321 such telephone companies in operation for at least ne year at the end of 1992. [FN22] According to the SBA's definition, such a mall business telephone company is one employing no more than 1,500 persons. FN23] All but 26 of the 2,321 wireline companies listed by the Census Bureau ere reported to have fewer than 1,000 employees. Even if all 26 of the emaining companies had more than 1,500 employees, there would still be 2,295 ireline companies that might qualify as small entities. Although it seems ertain that some of these carriers are not independently owned and operated, we re unable at this time to estimate with greater precision the number of wireline arriers and service providers that would qualify as small business concerns nder SBA's definition. Therefore, we estimate that fewer than 2,295 ommunications wireline companies are small entities that may be affected by hese rules.

FN22 1992 Census at Firm Size 1-123 (based on previous SIC codes).

FN23 13 CFR 121.201, North American Industry Classification System (NAICS) code 13310. The category of Telecommunications Resellers, NAICS code 513330 also has n associated business size standard of 1,500 or fewer employees.

40. Local Exchange Carriers, Competitive Access Providers, Interexchange arriers, Operator Service Providers, Payphone Providers, and Resellers. Neither he Commission nor the SBA has developed a specific size standard definition for mall LECs, competitive access providers (CAPS), interexchange carriers (IXCs), perator service providers (OSPs), payphone providers, or resellers. The closest pplicable size standard for these carrier-types under SBA rules is for wired elecommunications carriers and telecommunications resellers. [FN24] The most eliable source of information that we know regarding the number of these arriers nationwide appears to be the data that we collect annually in connection ith the TRS. [FN25] According to our most recent data, there are 1,329 LECs, 532 APs, 229 IXCs, 22 OSPs, 936 payphone providers, and 710 resellers. [FN26] lthough it seems certain that some of these carriers are not independently owned nd operated, or have more than 1,500 employees, we are unable at this time to stimate with greater precision the number of these carriers that would qualify s small business concerns under the SBA's definition. Therefore, we estimate hat there are fewer than 1,329 small entity LECs or small incumbent LECs, 532 APs, 229 IXCs, 22 OSPs, 936 payphone providers, and 710 resellers that may be ffected by these rules.

FN24 13 CFR 121.201, NAICS codes 513310 and 513330.

FN25 See 47 CFR 64.601 et seq.; Provider Locator at Table 1.

FN26 Provider Locator at Table 1. The total for resellers includes both toll

esellers and local resellers.
41. Wireless Carriers. The applicable definition of a small entity wireless arrier is the definition under the SBA rules applicable to radiotelephone wireless) companies. This provides that a small entity is a radiotelephone ompany employing no more than 1,500 persons. The Census Bureau reports that here were 1,176 radiotelephone (wireless) companies in operation for at least ne year at the end of 1992, of which 1,164 had fewer than 1,000 employees. FN27] Even if all of the remaining 12 companies had more than 1,500 employees, here would still be 1,164 radiotelephone companies that might qualify as small ntities if they are independently owned are operated. It seems certain that ome of these carriers are not independently owned and operated. Consequently, e estimate that there are fewer than 1,164 small entity radiotelephone companies hat may be affected by the actions taken in this Order on Remand.

FN27 1992 Census at Firm Size 1-123.
42. Cellular, PCS, SMR and Other Mobile Service Providers. The most reliable ource of current information from which we can draw an estimate of the number of mall business commercial wireless entities appears to be data the Commission ublished annually in its Trends in Telephone Service report. [FN28] According to he most recent Trends Report, 806 carriers reported that they were engaged in he provision of cellular service, PCS services, or SMR telephony services, which re placed together in the data. [FN29] Moreover, 323 such licensees in ombination with their affiliates have 1,500 or fewer employees and thus qualify s "small businesses" under the above definition. Thus, we estimate that there re 323 or fewer small wireless service providers that may be affected by the ules we adopt in this proceeding.

FN28 Trends in Telephone Service, Common Carrier Bureau, Industry Analysis ivision (Aug. 2001) ("Trends Report"). This report is available on-line at: ttp://www.fcc.gov/Bureaus/Common_Carrier/Reports/FCC-State_ Link/IAD/ rend801.pdf

FN29 Trends Report, Table 5.3.

D) Description of Projected Reporting, Recordkeeping and Other Compliance equirements.

43. No reporting and recordkeeping requirements are imposed on elecommunications carriers. Telecommunications carriers, including small arriers, will have to upgrade their network facilities to provide to law nforcement the assistance capability requirements adopted herein. Although ompliance with the technical requirements will impose costs on carriers, we have xamined means by which these costs will be minimized (such as by federal cost- eimbursement mechanisms and the ability of carriers to charge for the provision f assistance capability services). The most detailed and reliable cost stimates for carriers to implement the assistance capability features we require erein are $159 million total for wireless carriers and $117 million for wireline arriers, including small entities. However, as discussed in paragraph 65,

upra, we expect the actual costs borne by carriers to be substantially lower fter the application of the cost-minimization provisions discussed above.

E) Steps Taken To Minimize Significant Economic Impact on Small Entities and ignificant Alternatives Considered.

44. The need for the regulations adopted herein is mandated by Federal egislation. In the regulations we adopt, we affirm our proposals in the Further PRM to establish regulations for wireline, cellular, and broadband PCS elecommunications carriers. Costs to telecommunications carriers will be itigated in several ways. For example, the final regulations require elecommunications carriers to make available to law enforcement call identifying nformation when it can be done without unduly burdening the carrier with network odifications, thus allowing cost to be a consideration in determining whether he information is "reasonably available" to the carrier and can be provided to aw enforcement. Thus, compliance with the assistance capability requirements of ALEA will be reasonable for all carriers, including small carriers. Also, under ALEA, some carriers will be able to request reimbursement from the Department of ustice for network upgrades to comply ***22007** with the technical requirements dopted herein, and others may defer network upgrades to their normal business ycle.

45. We believe that these provisions can serve to mitigate any additional cost urdens that would otherwise be borne by small carriers. The Commission onsidered several alternatives advanced by commenters in the proceeding--ncluding not requiring the assistance capabilities adopted herein--but rejected hem after concluding that they would not meet the statutory requirements of ALEA. We note that the statutory mandate under CALEA requires all carriers to rovide assistance capabilities, and this includes small entities. Thus, we must ely on cost-mitigation procedures to address NTCA's assertion that any egulation that requires carriers to deploy or upgrade facilities will isproportionally affect small carriers.

eport to Congress

46. The Commission will send a copy of this Supplemental FRFA, along with this rder on Remand, in a report to Congress pursuant to the Congressional Review ct, 5 U.S.C. 801(a)(1)(A). In addition, the Commission will send a copy of this rder on Remand, including this Supplemental FRFA, to the Chief Counsel for dvocacy of the Small Business Administration. A copy of this Order on Remand, ncluding the Supplemental FRFA, will also be published in the Federal Register. ee 5 U.S.C. 604(b).

rdering Clauses

47. Authority for issuance of this Order on Remand is contained in sections 1, , 229, 301, 303, and 332 of the Communications Act of 1934, as amended, and ection 107(b) of the Communications Assistance for Law Enforcement Act, 47 .S.C. 151, 154, 229, 301, 303, 332, and 1006(b).

7 FR 21999-01
Cite as: 67 FR 21999, *22007)

48. The Commission's Consumer and Governmental Affairs Bureau, Reference nformation Center, shall send a copy of this Order on Remand, including the upplemental Final Regulatory Flexibility Analysis, to the Chief Counsel for dvocacy of the Small Business Administration.

ist of Subjects in 47 CFR Parts 22, 24 and 64

Communications common carriers.
Federal Communications Commission.

arlene H. Dortch,

ecretary.

ules Changes

For the reasons discussed in the preamble, the Federal Communications Commission mends 47 CFR parts 22, 24 and 64 as follows:

ART 22--MOBILE SERVICES

1. The authority citation in part 22 continues to read:

Authority: 47 U.S.C. 154, 222, 303, 309 and 332.

2. Section 22.1102 is amended by adding definitions in alphabetical order to ead as follows:

22.1102 Definitions.

* * * *
Destination. A party or place to which a call is being made (e.g., the called arty).
* * * *
Direction. A party or place to which a call is re-directed or the party or place rom which it came, either incoming or outgoing (e.g., a redirected-to party or edirected-from party).
* * * *
Origin. A party initiating a call (e.g., a calling party), or a place from which call is initiated.
* * * *
Termination. A party or place at the end of a communication path (e.g. the alled or call-receiving party, or the switch of a party that has placed another arty on hold).
* * * *
3. Section 22.1103 is amended by revising paragraph (b) and adding paragraph c) to read as follows:

22.1103 Capabilities that must be provided by a cellular telecommunications arrier.

* * * *

(b) As of November 19, 2001, a cellular telecommunications carrier shall provide o a LEA communications and call-identifying information transported by packet- ode communications.

(c) As of June 30, 2002, a cellular telecommunications carrier shall provide to LEA the following capabilities:

(1) Content of subject-initiated conference calls;

(2) Party hold, join, drop on conference calls;

(3) Subject-initiated dialing and signaling information;

(4) In-band and out-of-band signaling;

(5) Timing information;

(6) Dialed digit extraction, with a toggle feature that can activate/deactivate his capability.

ART 24--PERSONAL COMMUNICATIONS SERVICES

4. The authority citation in part 24 continues to read as follows:

Authority: 47 U.S.C. 154, 301, 302, 303, 309 and 332.

5. Section 24.902 is amended by adding definitions in alphabetical order to ead as follows:

24.902 Definitions.

* * * *

Destination. A party or place to which a call is being made (e.g., the called arty).

* * * *

Direction. A party or place to which a call is re-directed or the party or place rom which it came, either incoming or outgoing (e.g., a redirected-to party or edirected-from party).

* * * *

Origin. A party initiating a call (e.g., a calling party), or a place from which call is initiated.

* * * *

Termination. A party or place at the end of a communication path (e.g. the alled or call-receiving party, or the switch of a party that has placed another arty on hold).

* * * *

6. Section 24.903 is amended by revising paragraph (b) and adding paragraph c) to read as follows:

24.903 Capabilities that must be provided by a broadband PCS telecommunications arrier.

* * * *

(b) As of November 19, 2001, a broadband PCS telecommunications carrier shall rovide to a LEA communications and call-identifying information transported by acket-mode communications.

(c) As of June 30, 2002, a broadband PCS telecommunications carrier shall rovide to a LEA the following capabilities:

(1) Content of subject-initiated conference calls;

(2) Party hold, join, drop on conference calls;

(3) Subject-initiated dialing and signaling information;

(4) In-band and out-of-band signaling;

(5) Timing information;

(6) Dialed digit extraction, with a toggle feature that can activate/deactivate his capability.

ART 64--MISCELLANEOUS RULES RELATING TO COMMON CARRIERS

7. The authority citation for part 64 is revised to read as follows:

Authority: 47 U.S.C. 151, 154, 201, 202, 205, 218-220, and 332 unless otherwise oted. Interpret or apply sections 201, 218, 225, 226, 227, 229, 332, 48 Stat. 070, as amended. 47 U.S.C. 201-204, 208, 225, 226, 227, 229, 332, 501 and 503 nless otherwise noted. ***22008**

8. Section 64.2202 is amended by adding definitions in alphabetical order to ead as follows:

64.2202 Definitions.

* * * *

Destination. A party or place to which a call is being made (e.g., the called arty).

* * * *

Direction. A party or place to which a call is re-directed or the party or place rom which it came, either incoming or outgoing (e.g., a redirected-to party or edirected-from party).

* * * *

Origin. A party initiating a call (e.g., a calling party), or a place from which call is initiated.

* * * *

Termination. A party or place at the end of a communication path (e.g. the alled or call-receiving party, or the switch of a party that has placed another arty on hold).

* * * *

9. Section 64.2203 is amended by revising paragraph (b) and adding paragraph c) to read as follows:

64.2203 Capabilities that must be provided by a wireline telecommunications arrier.

* * * *

(b) As of November 19, 2001, a wireline telecommunications carrier shall provide to a LEA communications and call-identifying information transported by packet-mode communications.

(c) As of June 30, 2002, a wireline telecommunications carrier shall provide to a LEA the following capabilities:

(1) Content of subject-initiated conference calls;

(2) Party hold, join, drop on conference calls;

(3) Subject-initiated dialing and signaling information;

(4) In-band and out-of-band signaling;

(5) Timing information;

(6) Dialed digit extraction, with a toggle feature that can activate/deactivate this capability.

FR Doc. 02-10832 Filed 5-1-02; 8:45 am]

BILLING CODE 6712-01-P

67 FR 21999-01, 2002 WL 820189 (F.R.)
END OF DOCUMENT

Westlaw Download Summary Report for WENGER,ERIC A 5417937

Date/Time of Request:	Tuesday, December 27, 2005 13:34:00 Central
Client Identifier:	DOJ
Database:	DCT
Citation Text:	Slip Copy
Lines:	924
Documents:	1
Images:	0

Only the Westlaw citation is currently available.
United States District Court,S.D. New York.
In re APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER FOR DISCLOSURE OF TELECOMMUNICATIONS RECORDS AND AUTHORIZING THE USE OF A PEN REGISTER AND TRAP AND TRACE
No. 05 MAG.1763.

Dec. 20, 2005.

OPINION AND ORDER

GORENSTEIN, Magistrate J.
***1** On October 19, 2005, the Court granted an *ex parte* application from the Government seeking an order requiring a provider of cellular telephone service to produce, *inter alia,* information pertaining to the location of cell site towers receiving a signal from a particular cellular telephone for a period of 60 days. The Court's Order expired on December 18, 2005. Because at least three other district courts have concluded that the Government lacks statutory authority for applications relating to certain types of cell site data, the Court is setting forth the reasons it granted the application in this case. Subsequent to the issuance of the Order, the Court sought additional information and briefing from the Government regarding the application. In addition, the Court asked the Federal Defenders of New York, Inc. to appear as *amicus curiae.* The Court has greatly benefitted from the briefing provided by both sides.

I. *BACKGROUND*

Cellular telephones communicate by means of signals to cellular telephone towers, which are operated by the various commercial carriers that provide cellular telephone service. As a cell phone user moves from place to place, the cell phone automatically switches to the tower that provides the best reception. In this case, the Government's application sought information on a prospective basis regarding cell towers being signaled by a specifically identified cellular telephone. The application, which remains under seal, furnishes detailed information indicating that the user of the target cellular telephone is engaged in ongoing criminal activity involving the illegal sale of contraband and that a warrant for the arrest of this person is outstanding. An order was previously granted by another Magistrate Judge in this District for cell site information with respect to the same target telephone.

The relevant portions of the application seek, for a period of 60 days, "cell site activations" for the telephone. The application also seeks a directive that the provider of the service furnish a map showing cellular tower "locations/addresses, sectors and orientations" as well as "the physical address/location of all cellular towers in the specified market." In a portion of the application not relevant to the instant opinion, the application seeks numbers dialed, incoming numbers, call durations, and other information relating to the subscriber of the target cellular telephone. The application contains additional provisions requiring that the provider furnish certain assistance to the federal law enforcement agents necessary to comply with the requested court order.

While the application uses the term "cell-site activations," the Government has specified that it seeks "cell-site information concerning the physical location of the antenna towers associated with the beginning and termination of calls to and from a particular cellphone." *See* Letter to the Court from Thomas A.G. Brown, dated November 22, 2005 ("Gov't Letter"), at 10. This phrasing corresponds roughly to the information that in fact has been obtained by the Government in this District in the past with respect to cell site information. Under prior orders issued in this District, the Government has been able to obtain a list of each call made by the subject cell phone, along with a date, start time and end time. With respect to the beginning or end of the call (and possibly sometimes in between), there is a listing of a three-digit number assigned to a cellphone tower or base station. At least one cellular provider will give, in addition to the number of the tower, a digit ("1," "2" or "3") indicating a 120 degree "face" of the tower towards which the cell phone is signaling.

***2** In suburban or rural areas, towers can be many miles apart. The Court has examined a map of cellular towers of a provider in lower Manhattan, which is one of the areas more densely populated by towers. In this area, the towers may be anywhere

from several hundred feet to as many as 2000 feet or more apart.

The Court is aware of three cases that have considered the availability of cell site data: *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F.Supp.2d 747 (S.D.Tex.2005) ("Texas Decision"); *In the Matter of an Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information*, 396 F.Supp.2d 294 (E.D.N.Y.2005) ("EDNY Decision"); and *In re Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers (Sealed) and Production of Real Time Cell Site Information*, 2005 WL 3160860 (D.Md. Nov. 29, 2005) ("Maryland Decision"). These cases appear to involve requests for cell site information that go beyond both what has been sought in this case and what has actually been received by the Government pursuant to any cell site application in this District. First, the cell site information provided in this District is tied only to telephone calls actually made or received by the telephone user. Thus, no data is provided as to the location of the cell phone when no call is in progress. Second, at any given moment, data is provided only as to a single cell tower with which the cell phone is communicating. Thus, no data is provided that could be "triangulated" to permit the precise location of the cell phone user. Third, the data is not obtained by the Government directly but is instead transmitted from the provider digitally to a computer maintained by the Government. That is, the provider transmits to the Government the cell site data that is stored in the provider's system. The Government then uses a software program to translate that data into a usable spreadsheet.

II. *DISCUSSION*

The Government's application cites to two enactments: the statutes governing the installation of pen registers and trap and trace devices, 18 U.S.C. § § 3121-27 ("the Pen Register Statute"), and a provision of the Stored Wire and Electronic Communications and Transactional Records Access Act codified at 18 U.S.C. § 2703. We begin our discussion with the text of these statutes inasmuch as "[e]very exercise in statutory construction must begin with the words of the text." *Saks v. Franklin Covey Co.*, 316 F.3d 337, 345 (2d Cir.2003). "The plainness or ambiguity of statutory language is determined by reference to the language itself, the specific context in which that language is used, and the broader context of the statute as a whole." *Robinson v. Shell Oil Co.*, 519 U.S. 337, 341 (1997) (citations omitted). In general, if the statutory language is not ambiguous, the statute is construed according to the plain meaning of the words. *See, e.g., Greenery Rehab. Group, Inc. v. Hammon*, 150 F.3d 226, 231 (2d Cir.1998) (citing *Rubin v. United States*, 449 U.S. 424, 430 (1981)). We look to the legislative history and other tools of statutory construction only if the statutory terms are ambiguous. *Id.* (citing *Aslanidis v. United States Lines, Inc.*, 7 F.3d 1067, 1073 (2d Cir.1993)).

A. *Pen Register Statute*

***3** The Pen Register Statute is the statute used to obtain information on an ongoing or prospective basis regarding outgoing calls from a particular telephone (captured by a "pen register") and incoming calls (captured by a "trap and trace" device). These devices are more fully defined in 18 U.S.C. § 3127(3), (4). [FN1] A "pen register" is defined as a device that provides not merely the telephone number of a telephone call dialed from the subject telephone-the most common use of the term "pen register"-but also "signaling information" transmitted by the subject telephone itself or the "facility from which a wire or electronic communication is transmitted," 18 U.S.C. § 3127(3). The term "signaling information" was added by the USA PATRIOT Act in 2001. *See* Pub.L. No. 107-56, § 216(c)(2), 115 Stat. 272, 290 (2001). Prior to the enactment of the USA PATRIOT act, the District of Columbia Circuit had held in connection with its interpretation of a related statute, 47 U.S.C. § 1001(2), that because a cell phone sends "signals" to cellphone towers in order to operate, the term "signaling information" includes information on the location of cell site towers used by a cellular telephone. *See United States Telecom. Ass'n v. FCC*, 227 F.3d 450, 458, 463-64 (D.C.Cir.2000). [FN2] While one cell site decision notes an absence of legislative history indicating that Congress intended cell site data to be included in this term when it enacted the USA PATRIOT Act, *see* Texas Decision, 396 F.Supp.2d at 761, the language enacted is not so limited. Indeed, the legislative history reflects that the language regarding "signaling information" would apply "across the board to all communications media." H.R.Rep. No. 107-236(I), 107th Cong., 1st Sess., *available at* 2001 WL 1205861, at *53 (Oct.

11, 2001). Accordingly, we will interpret this provision in accordance with its most obvious meaning and the one that naturally would have been available to Congress, through the *United States Telecom* case, when the statutory language was enacted in 2001. *See* Lorillard v. Pons, 434 U.S. 575, 581 (1978) ("Where ... Congress adopts a new law incorporating sections of a prior law, Congress normally can be presumed to have had knowledge of the interpretation given to the incorporated law, at least insofar as it affects the new statute.").

FN1. At one time, a "pen register" referred perforce to a physical device that recorded information regarding outgoing telephone calls. In this District at least, law enforcement agencies do not in all instances need to install a physical device on a telephone line to obtain information regarding these calls. Instead, information that was heretofore captured by a pen register can now be transmitted digitally by the telephone service provider. The Government has properly assumed that, despite this change in technology, it is bound to follow the Pen Register Statute to obtain information otherwise covered by the statute.

FN2. Because the location information is "transmitted" by the cell phone, a pen register (not a trap and trace device) identifies location information for both incoming and outgoing calls. *See* 18 U.S.C. § 3127(3).
On a separate point, *amicus* contends that the "signaling information" available under the Pen Register Statute is only the "signaling information" that is transmitted during a particular telephone call. *See* Letter to the Court from Yuanchung Lee, dated October 27, 2005 (*"Amicus* Letter") at 16. The statute is ambiguous on this point, however. It says only that a pen register records the "signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." 18 U.S.C. § 3127(3). The term "is transmitted" is susceptible of two meanings: it could refer either to a particular communication or to an ongoing transmission. It is not necessary to reach this issue, however, because here the Government has sought only cell-site information tied to telephone calls.

In addition, construing the pen register definition as covering the capture of cell site data is the only way to make sense of a separate statute: 47 U.S.C. § 1002. As described in the next section, that statute specifically assumes that cell site data is available under the Pen Register Statute.

Notably, the showing required to install a pen register is a low one: the Government need only identify the law enforcement agency conducting the investigation and certify that the information likely to be obtained is "relevant to an ongoing criminal investigation" being conducted by the agency. 18 U.S.C. § 3122(b)(1), (2). Orders requiring the installation of a pen register may not exceed 60 days, though they may be extended for additional 60-day periods if the required showing is made. 18 U.S.C. § 3123(c). In certain emergency situations, a pen register may be installed even in the absence of a court order. 18 U.S.C. § 3125. The Pen Register Statute explicitly excludes from its definition "the contents of any communication"-an exclusion not relevant to the instant application as there is no effort to obtain the contents of any telephone calls. *See* 18 U.S.C. § 3127(3).

***4** The Government has certified that the cell site information it seeks here is "relevant and material to an ongoing investigation." Thus, the Pen Register Statute would by itself provide authority for the order being sought by the Government were it not for a provision codified elsewhere in the United States Code. That provision occurs in an "exception" clause within 47 U.S.C. § 1002, which is entitled "Assistance capability requirements."

B. *47 U.S.C. § 1002*

Section 1002 was enacted as part of the Communications Assistance for Law Enforcement Act of 1994. It requires telecommunications carriers to ensure that their equipment is capable of providing a law enforcement agency with information to which it may be entitled under statutes relating to electronic surveillance. Section 1002 provides, in pertinent part, as follows:
a telecommunications carrier shall ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of-
* * *
(2) expeditiously isolating and enabling the

government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier-
(A) before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government); and
(B) in a manner that allows it to be associated with the communication to which it pertains,

except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of Title 18), such 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);

47 U.S.C. § 1002(a)(2) (emphasis added).

The phrase "information that may disclose the physical location of the subscriber" in the exception clause can reasonably be interpreted to encompass the prospective cell site information being sought by the Government here, although, as already discussed, the information the Government obtains in this District "disclose[s] the physical location" of the subscriber in only the roughest manner. [FN3]

> FN3. A literal reading of this exception clause might lead one to question whether it is of any relevance at all to the Government's application inasmuch as the clause is framed only as an exception to the sort of "capab[ilities]" a carrier is obligated to "ensure" that it possesses. Under this reading, the exception clause merely states that a carrier is not obligated to ensure that it possesses the capability to disclose physical location information. The clause says nothing about whether the carrier should or should not disclose such information. Nor does it say anything about whether the Government may obtain an order for such information. As is described below, however, the legislative history relevant to this provision reflects that a literal reading of this kind would be at odds with the intention of Congress.

The effect of the exception clause is not obvious at first glance. But the clause plainly reflects an underlying assumption that physical location data *would* have been obtainable under the Pen Register Statute in the absence of the exception clause. Otherwise, it would have been unnecessary to add the exception clause at all. Indeed, the legislative history of section 1002 states as much. *See* H. Rep. 103-827(I), reprinted in 1994 U.S.C.C.A.N. 3489, 3497, 1994 WL 557197, at *17 (Oct. 4, 1994) ("Currently, in some cellular systems, transactional data that could be obtained by a pen register may include location information."); S. Rep. 103-402, *available at* 1994 WL 562252, at *18 (Oct. 6, 1994) (same). [FN4]

> FN4. In fact, the definition of a "pen register" in effect at the time of the exception clause's passage did not seem to include cell site or location information, inasmuch as the term "pen register," prior to the USA PATRIOT Act amendment in 2001, had been defined as a device that identified "the number dialed or otherwise transmitted." *See* Pub.L. No. 99-508, § 301, 100 Stat 1848 (Oct. 21, 1986). Nonetheless, Congress obviously thought such information was available under the Pen Register Statute when the exception clause was enacted in 1994.

***5** But if the exception clause of 47 U.S.C. § 1002(a)(2) is read to mean that a pen register may not be used at all to deliver cell site information to the Government, then the Government may not acquire cell site information by *any* mechanism. This is because the Pen Register Statute is clear that the device that captures cell site information-that is, a "pen register"-may be installed only pursuant to the Pen Register Statute itself. As noted, the Pen Register Statute defines a pen register as a device that provides "signaling information" (*e.g.*, cell site information). *See* 18 U.S.C. § 3127(3). At the same time, the Pen Register Statute states unequivocally (with exceptions not relevant here) that "no person may install or use a pen register ... without first obtaining a court order under section 3123"-that is, pursuant to a court order issued under the Pen Register Statute itself. *See* 18 U.S.C. § 3121(a). Taken together, the two sections require that prospective cell site information may be obtained *only* pursuant to the Pen Register Statute. If the exception clause in 47 U.S.C. § 1002(a)(2) is read to mean that the Pen Register Statute may not be used in any form to obtain cell site information, as is urged by *amicus* and the other cell site cases, the exception clause in combination with section 3121(a) would constitute a directive that cell site information was

not obtainable by any mechanism at all.

Amicus and the other cell site cases do not address this question and simply assume that 47 U.S.C. § 1002(a)(2) means that some mechanism other than the Pen Register Statute may be used to obtain cell site information as long as this mechanism stands on its own-that is, as an independent ground authorizing the collection of cell site data. The cell site cases believe a search warrant under Fed.R.Crim.P. 41 is the appropriate mechanism, *see, e .g.,* Texas Decision, 396 F.Supp.2d at 757, and *amicus* asserts that it is the Title III wiretap statute, *see* Letter to the Court dated December 6, 2005 from Yuanchung Lee, at 5-6. But, again, this reading fails to give effect to the explicit directives contained in the Pen Register Statute that a pen register-which is defined to include a device providing cell site information-can be installed only pursuant to "a court order under section 3123 of [Title 18]." 18 U.S.C. § 3121(a). In other words, Fed.R.Crim.P. 41 or Title III cannot by themselves provide authority for the Government's application because any warrant or order issued pursuant to those mechanisms must necessarily authorize the installation of a "pen register."

If the cell site cases and *amicus* were correct in their interpretation of the exception clause-that is, that it constitutes a simple direction that no cell site information may be obtained pursuant to the Pen Register Statute-this Court might conclude that Congress intended that the Government could not obtain cell site information by any means. However, the exception clause in fact does not contain a direction that no cell site information may be obtained "pursuant" to the Pen Register Statute. Instead, it states that cell site information may not be obtained *"solely* pursuant" to the Pen Register Statute. 47 U.S.C. § 1002(a)(2). The phrase "solely pursuant" is an unusual one-so unusual that the only time it appears in the United States Code is in 47 U.S.C. § 1002(a)(2). [FN5]

> FN5. The phrase "only pursuant" appears several dozen times in the United States Code. But in each instance the phrase is used to direct affirmatively how an act is to be done-for example, to direct that judicial review of an order may be obtained "only pursuant" to a particular statutory provision. 49 U.S.C. § 46301(d)(7)(D)(iii). Here, however, the exception clause authorizes something to be done as long as it is *not* done "solely pursuant" to a particular statutory provision. Thus, the statutes using "only pursuant" provide no assistance in our interpretation.

***6** The use of the word "solely" is significant. "Solely" means "without another" or "to the exclusion of all else." *See Merriam-Webster's Collegiate Dictionary* (10th ed.2000), at 1114. If we are told that an act is not done "solely" pursuant to some authority, it can only mean that the act is done pursuant to that authority *"with* [ ] another" authority. *Id.* As a result, the use of the word "solely" in section 1002 necessarily implies that "another" mechanism may be combined-albeit in some unspecified way-with the Pen Register Statute to authorize disclosure of cell site information.

As just noted, *amicus* and the other cell-site cases read the exception clause as a direction to the Government to rely exclusively on some other mechanism to obtain the cell-site information and to rely on that other mechanism alone. We have already pointed out one problem with this reading-that it results in a contradiction in the terms of the Pen Register Statute and 47 U .S.C. § 1002. But there is a second problem, which is reflected in section 1002 itself. If section 1002 means that the Pen Register Statute cannot be relied on whatsoever to obtain cell site information, it would have been sufficient for the statute's drafters to use the word "pursuant" rather than the phrase "solely pursuant." In other words, the use of the word "pursuant" would have been enough by itself to give a clear direction that cell-site information cannot be obtained under the Pen Register Statute. Given the doctrine that "we must, if possible, construe a statute to give every word some operative effect," *Cooper Industries, Inc. v. Aviall Services, Inc.*, 125 S.Ct. 577, 584 (2004), the word "solely" must be given semantic content if it is possible to do so. The most reasonable reading of the word "solely" is that if cell-site information is not being obtained "solely" pursuant to the statute, it is being obtained pursuant to the opposite of "solely": that is, not "alone" but in combination with some other mechanism.

While we have extracted some semantic content out of the word "solely," it has hardly been a satisfying exercise inasmuch as we are left with the conclusion that Congress has given a direction that cell site information may be obtained through some unexplained combination of the Pen Register Statute with some other unspecified mechanism. As unsatisfying as this result is, the only alternative is either (1) to ignore the plain dictate of 18 U.S.C. §

3121(a) by assuming that 47 U.S.C. § 1002 means that some other mechanism may be used to intercept "physical location" information if it can do so on an independent basis, or (2) to ignore Congress's inclusion of the otherwise unnecessary word "solely" and conclude that ongoing cell site data is not obtainable at all.

We reject the first choice as it requires us to ignore a clear statutory command. Nor can we accept the second choice because it requires us to conclude that Congress intended that ongoing cell site location information could not be obtained by any means at all. Congress, however, plainly manifested its intention to the contrary. First, as noted, any such interpretation necessarily reads the word "solely" out of the exception clause. If Congress had intended that no prospective cell site data be obtainable, it would have simply said in the exception clause that physical location information could not be obtained "pursuant" to the Pen Register Statute.

*7 Second, the only legislative history that directly bears on the meaning of the exception clause-consisting of a prepared statement of former Federal Bureau of Investigation ("FBI") director Louis Freeh-reflects that the § 1002 exception was put in at the suggestion of the FBI itself, as a way of assuring Congress that the FBI would rely on mechanisms-referred to as "court orders and subpoenas"-other than the Pen Register Statute to obtain physical location information, including cell site data. *See Police Access to Advanced Communication Systems: Before the Subcommittee on Technology and the Law of the Committee on the Judiciary United States Senate and the Subcommittee on Civil and Constitutional Rights of the Committee on the Judiciary House of Representatives* (1994) (statement of FBI Director Louis J. Freeh) ("Freeh Statement"), *available at* 1994 WL 223962 ("Even when such generalized location information, or any other type of 'transactional' information, is obtained from communications service providers, court orders or subpoenas are required and are obtained."). Thus, it would not make sense for Congress to have taken Director Freeh up on his proposal by barring law enforcement agencies from obtaining cell site information entirely.

Third, the District of Columbia Circuit, in considering the "solely pursuant" exception in the context of a Federal Communications Commission's rule-making proceeding, approved of the FCC's decision that section 1002 "simply imposes upon law enforcement an authorization requirement different from that minimally necessary for use of pen registers and trap and trace devices." *United States Telecom Ass'n*, 227 F.3d at 463 (citing *In the Matter of Communications Assistance for Law Enforcement Act*, 14 F.C.C.R. 16794, 16815, ¶ 44 (1999)). The plain import of this statement is that law enforcement agencies would be able to get authorizations to obtain cell site information from some mechanism, although the Government would have to meet an authorization requirement different from the minimal standard provided in the Pen Register Statute.

Having rejected the two alternatives-that is, that cell site data can be obtained without reliance on the Pen Register Statute or that it is not obtainable at all-we are back at the originally discussed reading of the word "solely." We thus conclude that Congress expected physical location information-including cell site information-would be obtainable by the Government by using some mechanism in combination with the Pen Register Statute. The idea of combining some mechanism with as yet undetermined features of the Pen Register Statue is certainly an unattractive choice. After all, no guidance is provided as to how this "combination" is to be achieved. But, again, in light of the language used in section 1002, the Court believes that it is the only choice possible.

The next question is (1) whether the other mechanism relied on by the Government-18 U.S.C. § 2703-is an appropriate mechanism to "combine" with the Pen Register Statute, and (2) if so, how section 2703 should be "combined" with the Pen Register Statute. To answer these questions, we turn to an examination of section 2703.

C. *Section 2703*

*8 Section 2703 contains three main sections that authorize the Government to obtain records. Two are not relevant here: section 2703(a) authorizes disclosure of the contents of wire or electronic communications held by a "provider of electronic communication service" and section 2703(b) authorizes disclosure of the contents of wire or electronic communications in a "remote computing service ."

Section 2703(c)(1) -the section relied upon by the Government-provides that a "governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber

to or customer of such service (not including the contents of communications)," provided the Government "offers specific and articulable facts showing ... reasonable grounds to believe that ... the records or other information sought, are relevant and material to an ongoing criminal investigation" under 18 U.S.C. § 2703(d). A separate portion of section 2703 provides that basic subscriber information-such as name, address and duration of calls-need not even meet this threshold showing but is obtainable merely by subpoena. *See* 18 U.S.C. § 2703(c)(2). The Government may obtain additional information about a subscriber under 18 U.S.C. § 2703(c)(1)(B) as long as the "specific and articulable facts" standard is met.

The first question that arises is whether prospective cell site data is encompassed in the phrase "record or other information pertaining to a subscriber to or customer of [an electronic communication] service."

Certainly, prospective cell site data is "information," and it may also be said-in this District at least-to be in the form of a "record" inasmuch as cell site information is transmitted to the Government only after it has been in the possession of the cell phone company. Cell site data also "pertain[s]" to a subscriber to or customer of cellular telephone service. The remaining question is whether cellular telephone service constitutes an "electronic communication service." According to 18 U.S.C. § 2711(1), we must turn to 18 U.S.C. § 2510 for the definition of this term. Section 2510 defines an "electronic communication service" to mean "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

The phrase "electronic communication" is itself defined. Section 2510(12) provides that "electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." With the definition taken thus far, it would be plain that a user of a cellular telephone is a "customer of an electronic communication service" under section 2703(d) since the cellular telephone makes transmissions to a tower through an electromagnetic system. *See generally* http://www.fda.gov/cellphones/qa.html# 1 (wireless phones rely on radio-frequency energy, which is a form of electromagnetic energy).

***9** *Amicus* argues, however, that an exception contained in the definition of "electronic communication" in section 2510(12) is of importance here. *Amicus* Letter at 8. The exception states that an "electronic communication ... does not include ... any communication from a tracking device (as defined in section 3117 of this title)." 18 U.S.C. § 2510(12)(C). Section 3117 in turn defines a tracking device as "an electronic or mechanical device which permits the tracking of the movement of a person or thing." 18 U.S.C. § 3117(b).

Because a cellular telephone arguably has the capability of being a "device which permits ... tracking"-in addition to its normal voice and data transmission uses-we must determine if the tracking device exception to the definition of "electronic communication" means that a cellular telephone service subscriber is not in fact a "customer of an electronic communication service" under section 2703(c).

To understand the import of this exception, it is necessary to examine what "service" is being provided to the customer of a cellular telephone. This is because the term "electronic communication" is used in section 2703 to describe the sort of "service" that an individual subscribes to or is a customer of, and the Government may only obtain "records or other information" pertaining to such a person. Section 2510(15) says that the relevant service is a service that provides to users thereof the ability to "send or receive ... electronic communications." The exception in section 2510(12)(C) tells us only that "tracking" information is not considered to be an electronic communication. But this exception does not alter the fact that the cellular telephone *service* that the customer uses and to which the subscriber subscribes is nonetheless an "electronic communication service" under section 2510(15).

We next turn back to section 2703, which governs "information" pertaining to "customers and users" of electronic communications service. It is certainly the case that cell site or tracking information constitutes "information" pertaining to customers or users of electronic communications services. Thus, such cell site or tracking information comes within section 2703(c) and consequently is the sort of "information" that the Government may seek pursuant to an order under section 2703(d).

The objection to this reading, *see Amicus* Letter at 8-9, appears to be as follows: section 2703(c) governs information pertaining to electronic communication services. The definition of "electronic

communication" in section 2510(12)(C) excludes tracking information. Therefore, the Government cannot get under section 2703 the tracking information a cell phone provides.

The problem with this syllogism is that it assumes that the term "information" in section 2703(c) is limited by the definition contained in section 2510. In fact, section 2510 does not speak to the scope of the term "information" in section 2703. Rather, section 2510 speaks only to the meaning of the term "electronic communication service," which it defines broadly as a service that "provides to users thereof the ability to send or receive ... electronic communications." Thus, the term "electronic communications service" in section 2703(c) refers broadly to the "service" of providing users with the "ability to send or receive ... electronic communications." It does not refer to any one particular piece of information, such as cell site information, that might be obtainable from the device carried by the user of the service. While tracking information is not to be considered part of "electronic communications" pursuant to the exception contained in 2510(12)(C), this does not alter the fact that the cellular telephone service to which a cellphone customer subscribes necessarily comes within the definition of section 2510(15). After all, the service a cellular telephone company "provides to users" is the ability to make cellular telephone calls, not exclusively tracking information. Inasmuch as a service that provides cellular telephone capabilities is within section 2510(15), information pertaining to a subscriber to or customer of that "service" is obtainable under section 2703(c).

***10** In other words, information on the location of cell towers is not the "service" to which a cellular customer subscribes. Instead, the user subscribes to the voice-and perhaps data-transmission capabilities provided by the cellular carrier. Although tower location information may be a necessary ingredient for the operation of that service, the "service" to which the user subscribes is still the "electronic communication" capabilities of the cellular telephone. Section 2703(c) tells us broadly that the Government may obtain "information" pertaining to users of this sort of service. Cell site information is just one of many possible categories of "information" that pertains to users of this service. The exception in section 2510(12)(C) does not purport to limit the meaning of the term "information." [FN6]

FN6. There is potentially an independent reason why the exception clause in section 2510(12)(C) does not limit the Government's ability to obtain cell site information under section 2703. The exception clause points to section 3117 for the definition of a tracking device. Section 3117, however, is a statute that refers to a tracking device that has been "install[ed]" at the behest of the Government. 18 U.S.C. § 3117(a). Here, however, no tracking device has been "installed."

It may seem anomalous that the Government may obtain under section 2703 a particular category of information pertaining to a user of electronic communications that is excepted from the term electronic communications itself. But this is not surprising given the multiple purposes that the section 2510(12)(C) exception serves. The definitions in section 2510 apply across the board to (1) wiretaps; (2) section 2703 applications; and (3) Pen Register Statute applications. *See* 18 U.S.C. § § 2510 (introductory clause); 2711(1); and 3127(1). There is no suggestion in the structure of the statues that the section 2510(12)(C) exception was meant to limit in any way the "information" that the Government was entitled to get under section 2703(c).

In light of the analysis so far, section 2703(c)'s use of the term "information" would cover the prospective cell site data being sought here. At least some of the cell site cases recognize that the term "information" includes historical cell site information. *See* Texas Decision, 396 F.Supp.2d at 759 n. 16; EDNY Decision, 396 F.Supp.2d at 313; Maryland Decision, 2005 WL 3160860, at *4; *see also Amicus* Letter at 12. They question, however, whether cell site information not yet in existence at the time of the order-that is, prospective or what is colloquially referred to as "real time" data-may be included in the term "information."

The text of the statute itself contains no limitation of this kind. Some courts have pointed to the title of the chapter in which the statute appears-the "Stored Wire and Electronic Communications and Transactional Records Access"-as harboring some importance in this regard. *See* Texas Decision, 396 F.Supp.2d at 760. But this title is of limited significance for two reasons. First, it refers to types of data-"communications" and "records"-that are narrower than one of the actual terms in section 2703(c): "information." Second, and more significantly, even the data being obtained regarding the location of the cell phone is in fact "stored" by the carrier-at least in

this District. Cell site information is not obtained directly by the Government. Instead, it is transmitted to the Government only after it has come into the possession of the cellular telephone provider in the form of a record.

***11** The question of "historical" versus "real time" data is still of some significance, however. While the data the Government seeks can appropriately be characterized as "stored" or "historical" records by the time the Government gets possession of them, the Government wants that information on an ongoing basis. That is, it wants a continuing order for the cell phone company to provide the stored records in the future.

Amicus and the cell site cases have properly pointed to aspects of 2703 that make it unsuited to requiring the carrier to provide cell site data on an ongoing basis. *Amicus* Letter at 12. The two related statutes that plainly permit transmission of information to the Government on an ongoing basis-the Pen Register Statute and Title III-both contain limitations, 60 days and 30 days respectively, that cap the duration of any prospective orders. *See* 18 U.S.C. § 3123(c)(1); 18 U.S.C. § 2518(5). Section 2703, by contrast, contains no such time limitation. In a similar vein, the Pen Register Statute and Title III contain automatic sealing provisions, *see* 18 U.S.C. § 2518(8)(b) and 3123(d)(1)-provisions that are obviously important to the Government when obtaining ongoing information-whereas section 2703 does not.

These omissions, however, are understandable when considered in the context of the discussion presented thus far. *Amicus* and the cell site cases have conducted their analysis of section 2703 as an effort to determine whether Congress "intended" section 2703 to cover prospective cell site data. *See, e.g.,* Texas Decision, 396 F.Supp.2d at 760; *Amicus* Letter at 11-12. But there is no reason to believe that section 2703 was specifically enacted as the mechanism to cover such cell site data inasmuch as the Pen Register Statute professes to be the only statute that authorizes the installation of the device used to capture this sort of data, *i.e.* "signaling information." *See* 18 U.S.C. § 3121(a).

Section 2703, however, remains an appropriate candidate as a legal mechanism that could properly be "combined," as contemplated by 47 U.S.C. § 1002(a)(2), with the Pen Register Statute to obtain cell site locations. This is because the text of section 2703(c) covers the data the Government seeks here. The heart of the statute-granting authority to obtain "information" about cell phone customers-does not on its face contain any limitation regarding when such information may come into being. It is thus susceptible to an interpretation that the "information" sought might come into being in the future. Moreover, because cell site data in this District exists as a record before it is transmitted to the Government, the text of the statute does not prevent the Government from presenting daily or hourly (or even more frequent) applications to the Court to obtain historical cell site data. Thus, as a theoretical matter, the statute permits the Government to obtain cell site data on a continuing or ongoing basis even under a narrow reading of section 2703.

***12** The principal reason why the statute does not serve easily as a fully independent source of authority for providing such data is a structural one: the statute does not contain certain procedural features, such as a time limitation, that Congress has typically included in statutes that permit the gathering of ongoing information. But this is an understandable omission given that Congress envisioned a pen register as the mechanism that would be used to capture cell site data, and the Pen Register Statute contains the procedural features missing from section 2703. In other words, the Pen Register Statute contains the time limitation (and sealing) provisions that are tied to the very "device"-that is, the pen register-that Congress deemed necessary to obtain prospective cell site information. It is thus logical to conclude that these two statutes in combination contain the necessary authority contemplated by Congress in 47 U.S.C. § 1002.

Section 2703 is an appropriate mechanism to "combine" with the Pen Register Statute for yet another reason. As the District of Columbia Circuit recognized, and as is implicit from the statement presented by Director Freeh, the objection to using the Pen Register Statute alone for the purpose of obtaining cell site data was that it contained a "minimal[ ]" authorization requirement. *United States Telecom Ass'n,* 227 F.3d at 463 (citing *In the Matter of Communications Assistance for Law Enforcement Act,* 14 F.C.C.R. 16794, 16815, ¶ 44 (1999)). Thus, the District of Columbia Circuit concluded that the section 1002 exception "simply imposes upon law enforcement an authorization requirement different from that minimally necessary for use of pen registers and trap and trace devices." *Id.* Section 2703, by contrast, contains a higher authorization requirement than that required for a pen register. While the Pen Register Statute permits disclosure of information upon the mere showing that

the information likely to be obtained is "relevant to an ongoing criminal investigation" being conducted by the agency, 18 U.S.C. § 3122(b)(2), section 2703 requires the Government to offer "specific and articulable facts showing ... reasonable grounds to believe that ... the records or other information sought, are relevant and material to an ongoing criminal investigation." *See* 18 U.S.C. § 2703(d). Using section 2703 thus fulfills the apparent purpose of the section 1002 exception: to require something different from than the "minimal[ ]" authorization requirement imposed by the Pen Register Statute.

Of course, *amicus* and the cell site cases suggest that Fed.R.Crim.P. 41 or Title III are better mechanisms than section 2703 to obtain the cell site information. They rely on them, however, based in part on their belief that the non-pen-register mechanism for obtaining cell-site data must operate independently of the Pen Register Statute. [FN7] But once this proposition is rejected, section 2703 is a far more obvious source of authority since it covers the very sort of information that is being sought under the warrant. Its only failing is that it does not explicitly allow for the continuous release of such information. Certainly, Title III does not represent an appropriate fit for cell site information inasmuch as its purpose is to govern the interception of the "contents" of communications. *See, e.g.*, 18 U.S.C. § § 2510(4), 2511(1); *United States v. New York Tel. Co.*, 434 U.S. 159, 167 (1977) (pen registers not within Title III because they do not acquire the "contents" of communications).

FN7. Their reliance is also based on the belief that a cell phone is transformed into a "tracking device" when prospective cell site data is sought. For reasons discussed further in the next section, the requirements that attach to tracking devices are not relevant here.

***13** In sum, section 2703 is the most obvious candidate to be used in combination with the Pen Register Statute to authorize the ongoing collection of cell site information because it covers cell site information generally. Section 2703's absence of procedural provisions that typically attach to the transmission of ongoing information is explained by the fact that the pen register is the proper "device" to obtain cell-site information. Thus the Pen Register Statute's procedural provisions that are tied to such a device are appropriately combined with an application under section 2703 to obtain such information.

D. *Effect of the Fourth Amendment*

The only remaining question is whether the issuance of a court order for cell site information under section 2703 and the Pen Register Statute is unconstitutional because it violates the Fourth Amendment's prohibition against unreasonable searches and seizures. *Amicus* (and some of the cell site cases) discusses the issue in terms of whether the cell phone is a "tracking device" and whether a warrant grounded in probable cause is necessary for the installation of such a device. But the data being sought by the Government in this District is not what *amicus* believes it to be. The information does not provide a "virtual map" of the user's location. *Amicus* Letter at 24. The information does not pinpoint a user's location within a building. Instead, it only identifies a nearby cell tower and, for some carriers, a 120-degree face of that tower. These towers can be up to 10 or more miles apart in rural areas and may be up to a half-mile or more apart even in urban areas. Moreover, the data is provided only in the event the user happens to make or receive a telephone call. Thus, *amicus'* s reference to tracking devices and the cases considering this technology is not on point. [FN8]

FN8. The tracking device statute, 18 U.S.C. § 3117, is of no relevance at all because it provides no guidance on what showing must be made to install a tracking device. It states only that *"If* a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction." 18 U.S.C. § 3117(a) (emphasis added); *see also United States v. Gbemisola*, 225 F.3d 753, 758 (D.C.Cir.2000) ("section 3117 does not prohibit the use of a tracking device in the absence of conformity with the section"). Not only is the statute prefaced by a conditional clause, the statute itself contemplates that a tracking device may be installed merely pursuant to an "order"-that is, without a warrant and thus without a probable cause showing. And, of course, it contemplates the "installation" of a tracking device, which has not been sought here.

In any event, the case most strongly relied on by *amicus*, United States v. Karo, 468 U.S. 705 (1984), held only that the installation of a true tracking device without the knowledge of the person it was tracking must be the subject of a warrant if the device discloses its location inside someone's home and that information could not have been obtained by observation. 468 U.S. at 714; *cf.* United States v. Knotts, 460 U.S. 276, 282 (1983) (no warrant required where the installed tracking device reveals information observable from a public highway). Here, however, the Government does not seek to install the "tracking device": the individual has chosen to carry a device and to permit transmission of its information to a third party, the carrier. As the Supreme Court has held in the context of telephone numbers captured by a pen register, the provision of information to a third party does not implicate the Fourth Amendment. *See* Smith v. Maryland, 442 U .S. 735, 744 (1979); *see also* United States Telecom. Ass'n v. FCC, 227 F.3d at 459 (*"Smith'* s reason for finding no legitimate expectation of privacy in dialed telephone numbers-that callers voluntarily convey this information to the phone company in order to complete calls-applies as well to much of the information provided by the challenged capabilities.") (referring to information that included "antenna tower location"). *Amicus* argues that the information is not voluntarily conveyed because, unlike telephone numbers, location information is being transmitted even in the absence of a telephone call. *Amicus* Letter at 23 (citing Texas Decision, 396 F.Supp.2d at 756-57). The Court need not reach this question because the only information being sought by the Government here is information tied to an actual telephone call. [FN9]

FN9. *United States v. Forest*, 355 F.3d 942, 951 (6th Cir.2004), suggests in dictum that there might be a Fourth Amendment concern where a law enforcement agent purposely dialed the target cellphone in order to obtain location data. The court viewed such an act as demonstrating that the user was not voluntarily providing the cell site data. Here, we have no request to authorize such an act.

Conclusion

***14** The above analysis applies with respect to the instant Order, and is based upon the technology that is available to the Government in this District. Because the Court cannot know how that technology may change, it intends to identify specifically, in any future orders authorizing the provision of cell site information, the character of the information that may be provided by a carrier. Specifically, any such Order will make clear that it contemplates the production only of: (1) information regarding cell site location that consists of the tower receiving transmissions from the target phone (and any information on what portion of that tower is receiving a transmission, if available); (2) tower information that is tied to a particular telephone call made or received by the user; and (3) information that is transmitted from the provider to the Government. If the Government seeks to obtain other information, it should provide additional briefing on why such information is permissible under the relevant authorities.

S.D.N.Y.,2005.
In re Application of U.S. for an Order For Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace
Slip Copy, 2005 WL 3471754 (S.D.N.Y.)

END OF DOCUMENT

Department of Justice
EXECUTIVE SECRETARIAT
CONTROL SHEET

DATE OF DOCUMENT: 01/13/2003
DATE RECEIVED: 01/14/2003

WORKFLOW ID: 295116
DUE DATE:

FROM: The Honorable Michael Chertoff
Assistant Attorney General
Criminal Division
Washington, DC 20530

TO: DAG

MAIL TYPE: Action Memorandum

SUBJECT: Memo seeking DAG approval of the amendment to the USA's Manual regarding CRM's approval of pen registers and trap and trace applications involving the collection of Uniform Resource Locators (URLs).

DATE ASSIGNED
1/22/2003

ACTION COMPONENT & ACTION REQUESTED
For DAG signature.
Office of the Deputy Attorney General

INFO COMPONENT:

COMMENTS: 2/10/03: DAG approved and signed ltr on 2/6/03. Original signed package returned to CRm for dispatch. 1/22/03: EOUSA concurred. 1/17/03: CRM submitted revised package.

FILE CODE:

EXECSEC POC: Pat Morgan: 202-616-0081

Do: Mr. Downing - 2/11/03

4