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: