

United States Court of Appeals

FOR THE DISTRICT OF COLUMBIA CIRCUIT

Argued May 17, 2000 Decided August 15, 2000

No. 99-1442

United States Telecom Association, et al.,
Petitioners

v.

Federal Communications Commission and
United States of America,
Respondents

AirTouch Communications, Inc., et al.,
Intervenors

Consolidated with
99-1466, 99-1475, 99-1523

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. Ronese.

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 A. 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 proceed-

ing, 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 being used in the commission of the crime or are commonly used by the suspect. 18 U.S.C.

s 2518(3). The Electronic Communications Privacy Act of 1986 ("ECPA"), id. s 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. s 3127(3); trap and trace devices record telephone numbers from which incoming calls originate, much like common caller-ID systems, see id. s 3127(4). Although telephone numbers are not protected by the Fourth Amendment, see *Smith v. Maryland*, 442 U.S. 735, 742-45 (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. s 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 con-

ference 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. s 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.* s 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....

Id. s 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.* s 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. ss 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.* s 1006. The Act "does not authorize any law enforcement agency or officer" to dictate the specific design of communications equipment, services, or features. *Id.* s 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. s 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. s 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.* s 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 Associ-

ation ("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 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 p 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 pp 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 p 138. The four additions 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 pp 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 pp 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 pp 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 pp 83-89.

Two industry associations--the United States Telecom Association and the Cellular 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 by the Commission. 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. s 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. s 1006(b)(2); and (3) failed both to ensure that the capability requirements are implemented "by cost-effective methods," id. s 1006(b)(1), and to "minimize the cost of such compliance on residential ratepayers," id. s 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. s 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.

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 De-*

fense Council, Inc., 467 U.S. 837 (1984). We ask first "whether Congress has directly spoken to the precise question at issue." *Id.* at 842. 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. 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 construction of the statute." *Id.* at 843. At this stage of Chevron analysis, we afford substantial deference to the agency's interpretation of statutory language. See *id.* at 844.

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. s 1002(a)(2); 18 U.S.C. s 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 (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. s 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 p 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. s 3127(3) (emphasis added), and trap and trace devices record "the originating number of ... an electronic communication," *id.* s 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 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 (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. 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.

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. 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. According to the agencies, the Commission reasonably interpreted "call-identifying information" to include the punch list capabilities and antenna tower location information. 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 (1983). Because we agree with the latter argument, we need not address the Commission's plea for Chevron deference.

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). 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 p 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. s 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 p 74 ("Party join information appears to identify the origin of a communication; party drop, the termination of a communication; and party hold, the tempo-

rary 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.

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. s 1006(b). Although the Commission used its rulemaking power to alter the J-Standard, it identified no deficiencies in 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.* s 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 p 20, 16809 p 30. The Commission acknowledged that "these estimates ... do not represent all carrier costs of implementing CALEA," *id.* at 16809 p 30, yet it found them to

be "a reasonable guide of the costs to wireline, cellular, and broadband PCS carriers for CALEA compliance," id.

The Commission never explained how its Order would satisfy CALEA's requirements "by cost-effective methods." 47 U.S.C. s 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 p 66, 16828 p 75, 16829-30 p 82, 16832 p 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."

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 (1971), and rest on reasoned decision-making 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 (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 (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 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.

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. s 1006(b)(2), with respect to post-cut-through dialed digit extraction. This punch list capability requires carriers to electronically monitor 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. s 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. s 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 p 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. s 1006(b)(1), but also "protect the privacy and security of communications not authorized to be intercepted," id. s 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 p 123. Yet the Order requires carriers to make available all post-cut-through dialed digits--those that 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

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. s 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 p 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 p 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. 112, 115-16 (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 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 p 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 p 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 p 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

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 envel-

ope, 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 available for recording or decoding." Third Report & Order, 14 F.C.C.R. at 16818 p 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 packet-mode communications." *Id.* at 16817 p 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 p 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 p 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 packet-mode 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 p 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. s 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 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.

ordered.

So