FIRE WITH FIRE: HOW THE FBI SET TECHNICAL STANDARDS FOR THE TELECOMMUNICATIONS INDUSTRY UNDER CALEA

Jared J. Nylund

Signed into law by President Clinton in 1994, the Communications Assistance for Law Enforcement Act1 ("CALEA" or the "Act") was intended to better define the duties of telecommunications carriers in assisting law enforcement in administering authorized wiretaps. The Act provided for industry establishment of technical standards outlining specifications that bring various technologies and services into compliance with CALEA's assistance capability requirements.2 Following years of industry deliberation over the standards, which were accompanied by protests from law enforcement agencies and privacy advocates, the Federal Communications Commission ("FCC" or the "Commission") issued a report and order adopting the proposed industry standards along with several additional features requested by the Federal Bureau of Investigation ("FBI").3 The propriety of the Third Report and Order and the standards contained within it, are now the subject of consolidated petitions for review pending in the United States Court of Appeals for the District of Columbia Circuit.4 Federal wiretap law is thus experiencing new Fourth Amendment challenges, in addition to other growing pains accompanying CALEA implementation, as it expands to cover more recent telecommunications technologies and services.

This comment begins with an overview of the history of federal wiretap law. Then, after an introduction to CALEA and its structure, the paper discusses and analyzes the FCC's Third Report and Order containing the technical standards for assistance capability. Finally, the author advances a series of arguments in favor of upholding the Third Report and Order. These arguments are designed to address both the economic concerns of telecommunications industry participants and the potential implications for individual privacy. This comment casts the disputed technical standards as precisely what Congress intended when it enacted CALEA: specifications designed to preserve the ability of law enforcement to carry out authorized wiretaps in the face of increasingly complex telecommunications technology. The innovative concept of establishing industry standards to achieve such a purpose will be defended by emphasizing its implementation of forward-looking design specifications that, in practice, should perpetuate the peaceful coexistence and continuing harmonization of individual electronic privacy and legally authorized surveillance technology.

I. BACKGROUND

The Fourth Amendment of the Constitution of the United States of America guarantees:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no war-

---

American courts of law observed the common law for such and recording the petitioner’s words violated the privacy York statute allowing the use of electronic eavesdropping in fifty years had passed since the invention of the telephone, enforcement and public safety tool.” H.R. Rep. No. 103-827(1), enforcement officials have consistently testified been or is about to be committed). facts establish probable cause that the offense is being, has been or is about to be committed; such in a wiretap application order, facts tending to show that an offense is being, has been or is about to be committed)..

Wiretapping was not considered a search and seizure within the scope of the Fourth Amend-

5 U.S. Const. amend. IV.
6 See 18 U.S.C. §§ 2518(1)(b), (3)(a) (1999) (requiring, in a wiretap application order, facts tending to show that an offense is being, has been or is about to be committed; such an order will be issued only if a judge determines that the facts establish probable cause that the offense is being, has been or is about to be committed).
8 Olmstead v. United States, 277 U.S. 438, 462-63 (1928).
9 232 U.S. 383 (1914).
10 See id. at 391-92.
11 See Olmstead, 277 U.S. at 465-66 (noting that by 1928, fifty years had passed since the invention of the telephone, and holding that unauthorized wiretaps installed and monitored without entering the petitioners’ homes or office were neither searches nor seizures within the meaning of the Fourth Amendment). But see Berger v. New York, 388 U.S. 41 (1967) (invoking the Fourth Amendment to invalidate a New York statute allowing the use of electronic eavesdropping in criminal investigations by law enforcement officers); Katz v. United States, 389 U.S. 347, 355 (1967) (concluding that “[t]he Government’s activities in electronically listening to and recording the petitioner’s words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a ‘search and seizure’ within the meaning of the Fourth Amendment”). Federal prohibition officers in Olmstead gathered evidence of a conspiracy to import and distribute “intoxicating liquors” in violation of the National Prohibition Act by inserting wires along telephone lines leading from petitioners’ homes and their “chief office,” and transcribing incriminating conversations overheard by the officers. See Olmstead, 227 U.S. at 456-57.
12 See Katz, 389 U.S. at 352-53 (citing Olmstead, 277 U.S. at 457, 464-66 (noting various authorities that tend to support a real and personal property-oriented reading of “searches and seizures” and urging construction of the Constitution in light of its literal meaning at the time of its adoption)).
15 See 47 U.S.C. § 605. The statute then read, in pertinent part, “no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person.” Nardone v. United States, 302 U.S. 379, 381 (1937) (quoting § 605 of the Communications Act).
16 There were two cases bearing this title and both are relevant here. See Nardone v. United States, 302 U.S. 379 (1937); Nardone v. United States, 308 U.S. 338 (1939). Both of the Nardone cases dealt with the same criminal trial in which federal agents used evidence from wiretaps to gain convictions under the National Prohibition Act. The issue addressed in the first Supreme Court opinion was whether, in view of section 605, evidence gathered in this way was admissible in a federal criminal trial. After determining that procuring such evidence by federal agents was illegal, thus rendering the evidence inadmissible, the case was remanded to the district court. Soon afterward, in the context of another subsequent appeal, the Second Circuit recast the issue to encompass “every other use of the proscribed evidence.” Nardone, 308 U.S. at 339. In its second opinion, the Supreme Court responded by stating that a trial judge must allow “the accused to prove that a substantial portion of the case against him was a fruit of the poisonous tree.” Id. at 341. The Court also placed upon the government the defensive burden of demonstrating the independent origin of any allegedly tainted evidence. See id.
17 The Supreme Court noted in Berger that, by 1967, some states permitted their law enforcement officials to use wiretaps under certain conditions defined by statute or in the state constitution. See Berger, 388 U.S. at 48-49 n.4-5.
of wiretap law in the United States. Both opinions brought electronic eavesdropping\(^\text{18}\) within the definition of a Fourth Amendment search and seizure.\(^\text{19}\) These decisions overturned criminal convictions based on evidence gathered by the illegal use of electronic eavesdropping.\(^\text{20}\) In both cases the Court based its decision on the Fourth Amendment, probably because Section 605 of the Communications Act was then limited to telephone and telegraph communications.\(^\text{21}\) By thus incorporating electronic eavesdropping into the Fourth Amendment, the Supreme Court effectively updated the law to reflect the new technological reality.\(^\text{22}\)

Berger and Katz, however, were more than just "right to privacy" cases.\(^\text{23}\) The Berger Court invalidated a New York statute allowing the issue of warrants for "eavesdropping" because the statutory standards for obtaining a warrant did not meet the explicit constitutional requirement of "particularly describing the place to be searched, and the persons or things to be seized."\(^\text{24}\) The statute did not require law enforcement to describe the sought conversations with particularity. It allowed eavesdropping to continue for two months under a single warrant and provided a simple renewal procedure. It did not require termination of surveillance upon seizure of the desired conversation, and it did not require a showing of "exigent circumstances" to overcome the lack of notice inherent in eavesdropping.\(^\text{25}\) While Katz did not address a state eavesdropping statute, that opinion also focused on the proper procedure for obtaining a warrant and carrying out authorized surveillance.\(^\text{26}\) Both decisions addressed law enforcement concerns regarding the difficulty of investigating organized crime without wiretaps or electronic eavesdropping techniques.\(^\text{27}\) As Justice White noted in his Berger dissent, anyone putting a finger to the wind in 1967 should have noticed that such law enforcement concerns had gained enough legitimacy in Congress to inspire federal legislation capable of undermining the strict requirements for legal electronic surveillance established by the Berger majority.\(^\text{28}\)

The contemplated federal eavesdropping legislation was ultimately enacted as Title III of the Omnibus Crime Control and Safe Streets Act of 1968\(^\text{29}\) ("1968 Act"). Title III contained the wiretap provisions that remain the core of federal wiretap law today.\(^\text{30}\) While upholding the existing federal ban on wiretapping and expanding it to

---

\(^{18}\) "Eavesdropping" is treated as including any method used to overhear private conversations. See id. at 51–53. Wiretapping implicitly falls within that definition. See id. at 46. Yet a survey of state laws in 1967 revealed inconsistent statutory treatment of wiretaps and electronic eavesdropping devices. See id. at 47–49.

\(^{19}\) See id. at 51 (holding that "the use of electronic devices to capture [a conversation is] a 'search' within the meaning of the [Fourth] Amendment"); Katz, 389 U.S. at 353 (finding that the government, in listening to and recording petitioner's telephone conversations, had conducted a Fourth Amendment "search and seizure").

\(^{20}\) See Berger, 388 U.S. at 44–45; Katz, 389 U.S. at 348–49.

\(^{21}\) See Berger, 388 U.S. at 64; Katz, 389 U.S. at 359.

\(^{22}\) "The law, though jealous of individual privacy, has not kept pace with these advances in scientific knowledge." Berger, 388 U.S. at 49.

\(^{23}\) See Katz, 389 U.S. at 350 ("[T]he Fourth Amendment cannot be translated into a general constitutional 'right to privacy' . . . its protections go further, and often have nothing to do with privacy at all.").

\(^{24}\) U.S. CONST. amend. IV. See Berger, 388 U.S. at 58–60 (discussing the various shortcomings of the statute).

\(^{25}\) See Berger, 388 U.S. at 58–60.

\(^{26}\) See Katz, 389 U.S. at 354–59 (reviewing "'the procedure of antecedent justification . . . that is central to the Fourth Amendment" (quoting Osborn v. United States, 385 U.S. 923, 330 (1966))).

\(^{27}\) See Berger, 388 U.S. at 60–62. Appended to Justice White's lengthy dissent in Berger was an excerpt from a 1967 report by the President's Commission on Law Enforcement and Administration of Justice, entitled "The Challenge of Crime in a Free Society," which classified wiretapping and eavesdropping as indispensable to fighting organized crime. See id. app. at 119–29 (White, J., dissenting). Justice White felt that the electronic surveillance at issue in Berger was reasonable under the circumstances and that the Court had improperly used the case as a vehicle for resolving the many issues raised by official wiretapping and eavesdropping. See id. at 118 (White, J., dissenting). Although no direct mention of the challenge of investigating organized crime without electronic surveillance was made in Katz, it can be inferred that the FBI investigation at issue concerned organized crime. The facts of the case centered on a conviction for participation in a bookmaking conspiracy, after which the petitioner was compelled to testify under a grant of immunity before a federal grand jury concerning the charges involved. See Katz, 389 U.S. at 349 n.3. It also appears that the agents in Katz believed that they were carrying out their investigation in an entirely legal fashion. See id. at 352, 356. (characterizing the agents as deliberately abstaining from penetrating the confines of the telephone booth, in reliance on Olmstead).

\(^{29}\) See Berger, 388 U.S. at 112–18 (noting the numerous bills then before Congress, as well as House and Senate committee hearings contemplating federal wiretap and eavesdropping legislation).


\(^{30}\) See In Re Communications Assistance for Law Enforcement Act, Department of Justice and Federal Bureau of Investigation, Joint Petition for Expedited Rulemaking, CC Dkt. No. 97-213 at 6 (filed Mar. 27, 1998) [hereinafter DOJ/FBI Petition]. Indeed, the federal wiretap statute is still commonly
include other forms of electronic eavesdropping, the 1968 Act laid out a uniform procedure under which electronic eavesdropping would be authorized and conducted legally by law enforcement. A court order could be issued allowing the interception of the contents of wire or oral communications upon a showing of probable cause that a crime has been, is being or will be committed, and that "particular communications" regarding the crime will thereby be acquired. The application for the order had to show that ordinary investigative procedures had failed, would probably not succeed or would involve too much danger. Only those crimes listed at Section 2516 could be investigated in this manner. Each order had to limit the interception period to the shortest time necessary for seizure of the desired communication defined in the order. Furthermore, the order had to include a clause directing that the interception of communications not authorized for seizure would be minimized.

This "minimization" requirement in Title III has since been alleged to satisfy the "particularity" requirement of the Fourth Amendment. At a minimum, the required showing that normal investigative means are insufficient for a given factual scenario is reminiscent of the "exigent circumstances" required by the Berger Court to overcome a lack of prior notice. Still, the 1968 Act contained requirements that notice of the investigation had to be provided following the termination of the interception period. In addition, prior to any trial in which the contents of intercepted communications would be introduced as evidence, copies of the application and authorizing court order were to be provided to each party. The party against whom the evidence was offered could move to suppress it on the basis of illegal interception, the insufficiency of the authorizing order or the failure of the investigating officers to conduct their surveillance in a manner consistent with the scope of the order.

One necessary provision not included in the 1968 legislation was a means for law enforcement to compel the cooperation of telephone carriers that were reluctant or unwilling to lend the necessary technical support for a court-ordered wiretap. This potential oversight was brought to Congress' attention in 1970 by the United States Court of Appeals for the Ninth Circuit. Shortly thereafter, Congress added a provision to the statute requiring telephone carriers to provide "all information, facilities, and technical assistance necessary to accomplish the interception" authorized.

Telecommunications technology advanced significantly over the next fifteen years. In an attempt to keep pace with the proliferation of new services and technologies, Congress responded with the Electronic Communications Privacy Act of 1986 ("1986 Act"). This legislation expanded existing federal wiretap authority to other nonvoice "electronic communications" not generally accessible to the public. Also included was a new Chapter 121 in Title 18 of the United States

---

footnotes:

51 The 1968 Act explicitly covered both wire and oral communications. See 18 U.S.C. § 2511(1)(a) (1968). "Congress therein defined oral communication" as "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation." 18 U.S.C. § 2510(2) (1968).

52 The Senate Report noted the twin purposes of the 1968 Act: to protect communications privacy and to "define[s] on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized." S. Rep. No. 90-1097, at 66 (1968).


36 See 18 U.S.C. § 2518(3)(a), (c).

37 See id. at § 2518(3)(a), (c). See also 18 U.S.C. § 2516 (1999) (containing the exclusive list of suspected criminal activity—mostly felonies—for the investigation of which a wiretap may be authorized).

38 See id. at § 2518(3).

39 See e.g., James X. Dempsey, Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy, 8 ALB. L.J. SCI. & TECH. 65, 72 (1997).

40 See supra note 25 and accompanying text. See also S. Rep. No. 90-1097, at 66.


42 See 18 U.S.C. § 2518(9).


45 See Application of the United States, 427 F.2d 639, 643-44 (9th Cir. 1970).


48 Under the 1986 Act, "electronic communications" is defined as "any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelec-
Code, devoted entirely to "Stored Wire and Electronic Communications and Transactional Records Access."48 Additionally, Congress decided to enact a new uniform federal procedure governing the authorization and use of pen registers and trap-and-trace devices.49 The use of these devices is not governed by the Fourth Amendment, and they had been held to be outside the scope of the 1968 Act because of their inability to intercept the contents of communications.50 The 1986 Act generally prohibited their use, making exceptions for court-authorized law enforcement actions—a design similar to the existing uniform scheme covering wiretaps.51 In addition to individual privacy concerns, Congress' chief objective in enacting the 1986 Act was to eliminate the "[t]he lack of clear [legal] standards [governing the privacy of nonvoice communications that] may expose law enforcement officers to liability and . . . endanger the admissibility of evidence."52

II. THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT ("CALEA")53

Recognizing the continued explosion of new telecommunications technology since 1986,54 Congress responded to the widening gap between legal standards and technological facts by enacting CALEA.55 In so doing, Congress also achieved a new paradigm in wiretap and communications privacy legislation.56 Where the 1986 Act had merely echoed the existing requirement that a telecommunications carrier must provide any "assistance necessary to accomplish the interception,"57 CALEA outlines the specific responsibilities of a telecommunications carrier when confronted by an interception order.58 The ensuing battle over appropriate technical standards for industry-wide implementation of the assistance capability requirements set forth in Section
103 of CALEA has since raised the question of whether the Congressional mandate was specific enough.  

A. Responsibilities of Telecommunications Carriers

For purposes of CALEA, the definition of a telecommunications carrier includes any person or entity that transmits or switches wire or electronic interstate or foreign communications as a "common carrier for hire." Congress explicitly intended this definition to include cellular carriers, personal communications service ("PCS") providers, cable operators, and satellite-based service providers, as well as local exchange carriers, inter-exchange carriers and competitive access providers. In addition, the FCC has the authority to designate future providers of yet-to-be-developed local telephone exchange technologies and services as "telecommunications carriers" subject to CALEA. Yet information service providers are specifically excluded from the statutory definition.

CALEA requires that telecommunications carriers provide authorized law enforcement officers access to communications contents and identifying information expeditiously, unobtrusively and from a remote location without enabling access to any communication not authorized for interception. Carriers do not have to maintain the same capability for enabling access to private networks. Carriers are not responsible for the decryption of any communication that is encrypted using either an algorithm not provided by the carrier or an algorithm that the carrier does not have the ability to decrypt. On the other hand, a telecommunications carrier that is a commercial mobile service provider must identify the carrier providing mobile services to an adjacent service area when the subject of a CALEA intercept order leaves the original service area and is "handed off" to the adjacent carrier.

All court-ordered law enforcement access to communications and call-identifying information must occur simultaneously with transmission unless law enforcement agrees to receive it at another time. If access to call-identifying information has been authorized under a pen register, or trap-and-trace device order, no information regarding the physical location of the subscriber may be provided to law enforcement other than the telephone number. Finally, the telecommunications carrier must protect "the privacy and security of communications and call-identifying information not authorized to be intercepted."
Although it may be difficult to imagine a law enforcement agency informing a court that violations of this last mandate have occurred, any sustained failure to comply with CALEA could result in civil penalties to the carrier of $10,000 per day.\footnote{See \textit{47 U.S.C. § 1006(a)(1)-(2)}. This safe harbor provision does not allow a carrier to avoid the requirements of \textit{47 U.S.C. § 1002} in the absence of accepted technical standards.}

B. Developing Technical Standards for Implementation

Just as Congress charged the telecommunications industry with ensuring the privacy of its own networks, it also delegated the initial determination of technical standards for compliance with CALEA to industry participants.\footnote{See \textit{In Re Communications Assistance for Law Enforcement Act, Report and Order}, 14 FCC Rcd. 4151, at para. 20 (1999) (setting forth minimum system security and integrity requirements for compliance with Section 105 of CALEA) [hereinafter \textit{First Report and Order}].} In creating a safe harbor provision that allowed carriers to comply with the assistance capability requirements of CALEA simply by meeting the accepted industry standard, Congress hoped to encourage efficient implementation of those requirements.\footnote{The carrier must not only fail to comply with the requirements of CALEA, but there must also be no other reasonably available access to the communication (such as another carrier). \textit{See 18 U.S.C. § 2522(a); 47 U.S.C. § 1007(a)(1).} In addition, compliance must be reasonably achievable using available technology. \textit{See 47 U.S.C. § 1007(a)(2).} The court issuing the surveillance order must then order the carrier to make the necessary modifications to achieve compliance. \textit{See 18 U.S.C. § 2522(a).} Fines may only be imposed for violations of modification orders. The court must consider good faith efforts by the carrier to comply and any unreasonable effect that compliance may have on the carrier's ability to do business. \textit{See 18 U.S.C. § 2522(c)(1); 47 U.S.C. § 1007(b).} See \textit{47 U.S.C. § 1006(a)(2)}.}

Telecommunications carriers and equipment manufacturers, under the auspices of the Telecommunications Industry Association ("TIA"), thus began to craft these technical standards in 1995.\footnote{See \textit{In Re Communications Assistance for Law Enforcement Act, Further Notice of Proposed Rulemaking}, 13 FCC Rcd. 22632, at para. 11 (1998) [hereinafter \textit{FNPRM}]. See also \textit{U.S. Government Report and Order}, Notice of Proposed Rulemaking, 13 FCC Rcd. 3149, at para. 12-13 (1997) [hereinafter \textit{FPRM}]. See also \textit{In Re Communications Assistance for Law Enforcement Act, Report and Order}, 14 FCC Rcd. 4151, at para. 20 (1999) (setting forth minimum system security and integrity requirements for compliance with Section 105 of CALEA) [hereinafter \textit{First Report and Order}].} The development of the standards so far has been concerned primarily with wireline, cellular and broadband PCS carrier compliance. At first, suggestions from law enforcement agencies were welcome.\footnote{See \textit{47 U.S.C. § 1006(a)(3)}.}

In 1997, the TIA submitted its draft standard for balloting with the American National Standards Institute ("ANSI").\footnote{See \textit{In Re Communications Assistance for Law Enforcement Act, Notice of Proposed Rulemaking}, 13 FCC Rcd. 3149, at para. 44 (1997) [hereinafter \textit{CALEA NRM}]. See also \textit{USTA Brief supra note 4}.} However, the draft standard was voted down with unanimous opposition from law enforcement.\footnote{See id. at para. 12. Industry members, law enforcement agencies and any other interested parties could participate in balloting. See id. at n.28.} Attached to the FBI's ballot was a list of eleven technical capabilities not included in the industry's draft standard that the FBI believed to be mandated by CALEA.\footnote{See \textit{In Re Communications Assistance for Law Enforcement Act, Further Notice of Proposed Rulemaking}, 13 FCC Rcd. 22632, at para. 11 (1998) [hereinafter FNPRM]. See \textit{id. supra note 4} at para. 15.} Later reduced to nine items, this list became known as the FBI "punch list."\footnote{See id. at para. 12-13.} After a few revisions to the standard, none of which included punch list items, the TIA decided to circumvent ANSI and another law enforcement veto by rebaloting the revised draft standard under its own procedures as an "interim standard."\footnote{See \textit{id. supra note 4} at para. 14 n.35, para. 15.} Following unanimous approval of the interim standard by industry ballots, the TIA and Committee T1\footnote{Committee T1 is the wireline standards-setting body sponsored by the Alliance for Telecommunications Industry Solutions. See \textit{id. supra note 4} at para. 14 n.35, para. 15.} jointly published interim standard J-STD-025, Lawfully Authorized Electronic Surveillance (the "J-standard"). TIA and Committee T1 then adopted it as the accepted standard defining technical services, features and interfaces to satisfy the...
safe harbor provisions of CALEA.83

Appreciating the likelihood of such a disagreement occurring between law enforcement and the telecommunications industry, Congress explicitly provided for mediation in the form of an FCC ruling upon the petition of "a Government agency or any other person [who] believes that [the adopted industry] standards are deficient."84 Among the petitions for rulemaking filed with the Commission under Section 107(b) of the Act85 was one filed jointly by the FBI and the Department of Justice ("DOJ").86 While the DOJ/FBI Petition generally lamented the under-inclusiveness of the J-standard, another petition for rulemaking filed one day earlier by the Center for Democracy and Technology ("CDT") maintained that the standard was over-inclusive and that compliance with it was not reasonably achievable.87 Closing the triangle was a petition filed by the TIA, asking the Commission to resolve the dispute over the J-standard's completeness. TIA also asked the Commission to establish a permanent standard on an expedited basis and to "remand any further technical standardization work to TIA."88 The Commission responded with a Further Notice of Proposed Rulemaking ("FNPRM") under its rulemaking authority granted by sections 107(b) and 301(a) of CALEA.89 In its FNPRM, the Commission made tentative conclusions regarding whether two contested features of the J-standard and the nine punch list items each satisfied the assistance capability requirements of the Act.90 It further stated that the uncontested technical requirements of the J-standard were "beyond the scope of this proceeding," and that any necessary modifications to the J-standard made by the Commission should be implemented by TIA.91 Finally, the FNPRM also sought opinions regarding the proper interpretation of the phrase "reasonably available" as it pertained to call-identifying information delivered under intercept authority authorized by Section 103.92

III. THIRD REPORT AND ORDER

At the end of August 1999, the Commission released its Third Report and Order93 that set out technical standards for compliance with CALEA's assistance capability requirements.94 In addressing the concerns of numerous groups regarding the issues discussed in the FNPRM, the Third Report and Order essentially adopted the J-standard plus six of the nine punch list items requested by the FBI.95 The Commission also therein defined "reasonably available" to refer to call-identifying information that is "present at an IAP and can be made available without the carrier being unduly burdened with network modifications."96

A. Location Information

One of the most hotly debated features of the J-standard is its inclusion of location information that, if available at a given IAP, can provide the "mobile terminal" location being used by the subject of the intercept order.97 In this regard, the Third Report and Order refers specifically to the statutory definition of "call-identifying information," which includes information identifying the origin, direction, destination or termination of a commu-

---

83 See id. at para. 15.
84 47 U.S.C. § 1006(b).
86 See DOJ/FBI Petition, supra note 30.
87 See FNPRM, 13 FCC Rcd. at para. 18–19.
88 Id. at para. 20.
89 See id. at para. 23. Sections 107(b) and 301(a) are codified at 47 U.S.C. §§ 1006(b) and 229(a), respectively. The former provision authorizes rulemaking specifically in response to petitions for rulemaking filed under 47 U.S.C. § 1006(b). The latter authorizes the Commission to "prescribe such rules as are necessary to implement the requirements of CALEA." 47 U.S.C. § 229(a).
91 Id. at para. 45, 132–33.
93 See FNPRM, 13 FCC Rcd. at para. 45.
94 Id. at para. 1. The standards adopted in the Third Report and Order only apply to wireline, cellular and PCS carri-
95 See id.
96 Id. at para. 29. An "IAP"—intercept access point—is defined in the J-standard as "a point within a telecommunication system where some of the communications or call-identifying information of an intercept subject's equipment, facilities and services are accessed." Id. at para. 14 (quoting J-STD-025 § 4.2.2). In other words, it is the physical point at which the line is tapped, which is usually a switch. See id. at para. 28 n.65. The J-standard more narrowly defines "reasonably available" as "present at an intercept access point for call processing purposes." Id. at para. 28 (emphasis added) (citing J-STD-025 § 4.2.1).
97 See id. at para. 37. The approval of this feature of the J-standard is one of the primary issues presented by the USTA, CTIA and CDT in their petition for review of the FCC's Third Report and Order. At publication this appeal was pending in the United States Court of Appeals for the District of Columbia Circuit. See USTA Brief, supra note 4.
nication. The Commission determined that the Act mandates the inclusion of certain location information as call identifying because it includes "origin" and "destination" in the statutory definition of call-identifying information. The Commission limited such location information to call site identification with regard to wireless communications, drawing an analogy to street address information already available to law enforcement for wireline telephone numbers. In response to CALEA's provision limiting location information acquired under pen register or trap-and-trace authority to "what may be determined from the telephone number," the Commission adopted the DOJ/FBI position that this provision does not entirely preclude location information from being "call-identifying information." Rather, the authorization requirements for law enforcement to gain access to such information are much stricter than those imposed on pen register and trap-and-trace device authorization.

B. Packet-Mode Communication Contents

The second contested feature of the J-standard is its failure to define a technical standard for separating the contents of packet-mode communications from the "call-identifying information" that would theoretically be available to law enforcement even under pen register authority. Such an omission could presumably make the entire communication accessible to law enforcement regardless of the level of authorized surveillance. Recognizing the difficulty of defining any uniform assistance capability standard for the numerous existing packet-mode technologies, particularly given their rapidly evolving nature, the Commission requested that TIA further study the matter and report its findings by September 30, 2000. The Commission then adopted the existing J-standard as an interim standard, potentially making available to law enforcement both call contents and call-identifying information under the authority required for a pen register by September 30, 2001.

C. FBI Punch List

The Commission's FNPRM tentatively addressed nine punch list items that the DOJ and FBI believe are mandated by CALEA but were not addressed in the J-standard. In the Third Report and Order, five of the punch list items were held to be within the scope of CALEA's definition of "call-identifying information" (at least under certain circumstances) and thus included in the assistance capability requirements of Section 103. These five items are (as further discussed below) information regarding: 1) party hold, join and drop on conference calls; 2) subject-initiated dialing and signaling; 3) in-band and out-of-band signaling; 4) call timing; and 5) dialed digit extraction (or "post-cut-through" digits). Another of the punch list items (contents of subject-initiated conference calls) was defined as a communication "to or from the equipment, facilities, or services of

---

98 See Third Report and Order, 14 FCC Rcd. at para. 44 (quoting 47 U.S.C. § 1001(2)).
99 See id.
100 See id. at para. 44–45.
102 See Third Report and Order, 14 FCC Rcd. at para. 44.
103 See id. at para. 47 n.97 (quoting J-STD-025 § 3). Some examples of packet-mode services are Integrated Services Digital Network ("ISDN"), Code Division Multiple Access ("CDMA"), Time Division Multiple Access ("TDMA"), Asynchronous Transfer Mode ("ATM") and Internet Protocol ("IP") services. See id. at para. 55 n.106. Traditional local wireline telephone service, where the entire two-way communication passes through the same path, is described as "circuit-mode." See id. at para. 47 n.97.
104 In supporting its ruling, the Commission assigned greater weight to the cost-minimization and innovation-encouraging factors of 47 U.S.C. § 1006(b)(1)–(5) (listing factors to be considered by the Commission when exercising its rulemaking authority) than it did to the privacy-protection factor. The Commission noted "independent legal barriers" that existed to using illegally obtained communications in court proceedings. See Third Report and Order, 14 FCC Rcd. at para. 56 (referring to 18 U.S.C. §§ 2515, 2518.).
105 See FNPRM, 13 FCC Rcd. at para. 13, 32.
106 See id. at para. 13, 32.
107 See Third Report and Order, 14 FCC Rcd. at para. 74, 82, 89, 95, 119.
108 See id.
a subscriber" and thus an authorized interception under CALEA. By contrast, the Commission rejected requirements for continuity check tones and the provision of surveillance and feature status information, which were the remaining three punch list items requested by the FBI. The Commission rejected these requirements because it held that they fell outside the Act's specific mandate.

1. Content of Subject-Initiated Conference Calls

The Commission adopted a practical approach to this FBI punch list item: it interpreted CALEA to allow the authorized surveillance of all conference call contents reasonably available at the intercept access point ("IAP") from which the subject is monitored. Citing provisions of CALEA Section 103 pertaining to "mobile service assistance requirements," however, the Commission concluded that a separate order would be required to enable law enforcement agencies to gain full access to contents of subject-initiated conference calls supported by the services of a remote carrier. The Third Report and Order does not require carriers to provide law enforcement with access to conference communications that are not available on the carriers' own equipment. Nor is any carrier required to provide law enforcement with access to conference call conversations that continue after the subject has terminated his or her connection—regardless of the service supporting the communication.

2. Party Hold, Join and Drop On Conference Calls

This second punch list item refers to a network signal generated by the equipment or service hosting a conference call. It effectively identifies individual parties as each connects to and disconnects from a conference call, or when one or more conference call participants are put on hold. Although such signals are not currently available everywhere, the Commission determined that they were "call-identifying information" within the scope of Section 103 and thus required if the conference call uses the carrier's facilities, equipment or services. The Commission held that "party join" and "party drop" signals identified the origin and termination of a communication, respectively, bringing both signals within the scope of CALEA section 102. On the other hand, the Commission found that "party hold" signals were information regarding the "temporary origin, temporary termination, or re-direction of a communication." The Commission determined that access to "party hold" signals, as a group, was necessary for law enforcement to monitor accurately the contribution to a conference call made by the subject of a wiretap order, as well as to minimize interception of communications not involving the subject.

3. Subject-Initiated Dialing and Signaling

When the subject of law enforcement surveillance activates carrier-provided service features

---

112 See id. at para. 66–67. Since the conference call is hosted by the telecommunications carrier to which the wiretap subject subscribes, law enforcement can monitor the contents of conversations among other parties to the conference call even if the wiretap subject puts the conference call on hold. See id. at para. 66. Therefore, if the conference call is hosted by another carrier's equipment, only those portions of the call in which the subject is participating will be accessible at the IAP. This may become relevant if the subject does not initiate the conference call or if the "conference bridge" for a subject-initiated conference call is located remotely—as is possible with some on-demand conference services. See id. at para. 67. Here, the Commission's refusal to require that a carrier's assistance continue after the communication has been given to another carrier is consistent with its treatment of wireless communications assistance when a wiretap subject has left the carrier's service area. See discussion supra note 68.
113 See id. at para. 67 n.129 (citing 47 U.S.C. §§ 1002(a)(1), (d)).
114 See id. at para. 67.
115 See id. at para. 67 n.129.
116 See id. at para. 68.
117 See id. at para. 75. The Commission found that party hold, join and drop signals were "reasonably available" within the meaning of 47 U.S.C. § 1002(a)(2). The Commission thus required the hosting carrier to provide law enforcement access to these signals, even in situations where these signals are not currently generated. See id. Presumably, this access includes services provided by a carrier's subcontractors. See id. at para. 71 (recognizing that Bell Atlantic raised this issue). However, no such network signals are required if the conference services are provided by equipment located on a customer's premises because no signals are generated by the carrier's network itself. See id. at para. 75.
118 See id. at para. 74. See also 47 U.S.C. § 1001(2) (including in the definition of "call-identifying information" signals that identify "the origin . . . or termination" of a communication).
119 Third Report and Order, 14 FCC Rcd. at para. 74.
120 See id.
such as call hold, call transfer, call forwarding, call waiting, or adding and dropping parties to a conference call, the Commission has held that notification of such activation is "call-identifying information" mandated by the assistance capability requirements of CALEA. These signals can be distinguished from party hold, join and drop signals because they only cover functions initiated by a surveillance subject and include services used in conjunction with nonconference calls. Like party hold, join and drop signals, these signals were held by the Commission to identify the origin, direction, destination or termination of a call. The Commission, therefore, requires that carriers provide law enforcement with access to these signals because they are necessary for law enforcement to associate other call-identifying information with the correct communication. However, subject-initiated dialing and signaling is not "readily available" to a carrier if processed by equipment located on a customer's premises, which means that the production of such privately generated information cannot be compelled.

4. In-Band and Out-of-Band Signaling

The Commission found some in-band and out-of-band signaling to be included in the CALEA definition of "call-identifying information." Therefore, to the extent that such signals sent by the carrier's equipment or services to the subscriber—such as call waiting notification, new voice mail notification, busy signal and ringing tone—pass through the IAP, they are "readily available" and thus required for law enforcement access under CALEA Section 103. As with party hold, join and drop, and subject-initiated dialing and signaling, any signal generated on-premises by customer equipment is not "reasonably available" and thus is not a required law enforcement assistance capability.

5. Timing Information

The Third Report and Order imposes a requirement on telecommunications carriers for time stamps on all transmissions to law enforcement agencies delivered pursuant to an interception order. The Commission considered the time stamp itself to be "call-identifying information" within the meaning of both sections 102 and 103 of CALEA. Furthermore, the Commission established a maximum delivery time of eight seconds for call-identifying information, beginning when the information is received at the IAP.

6. Surveillance Status

Periodic surveillance status information, which would theoretically include updated wiretap activity and functionality data, was held by the Commission to be outside of the scope of necessary assistance capability requirements under CALEA.

---

121 See id. at para. 82. The Commission found that subject-initiated dialing and signaling, including dialed digits, depressed or released on-hook buttons and use of flash buttons, were "readily available" to the extent that these signals were processed at the IAP. See id.

122 See id. at para. 81. Party hold, join and drop signals (as referenced in the second punch list item) contain information relating to all parties to a conference call—not just the subject of a wiretap order. Subject-initiated dialing and signaling, while containing some overlapping information, focuses instead on all signals generated only by the subject of a wiretap order, whether or not he or she is in a conference call. See id. (discussing the DOJ/FBI reply comments to BellSouth's suggestion that information from such signals would be redundant).

123 See id. at 82 (referring to 47 U.S.C. §§ 1001(2) (defining "call-identifying information") and 1002(a)(2)(B) (identifying capability requirement for associating call-identifying information with call content)). An example presented in the Third Report and Order features a hypothetical law enforcement officer becoming confused as to which communication matches which call-identification information when a subject activates his or her call waiting in order to answer another call. See id.

124 See discussion supra note 117. See also Third Report and Order, 14 FCC Rcd. at para. 82.

125 See Third Report and Order, 14 FCC Rcd. at para. 89. The Commission supported this finding by noting that such signaling indicates "information about the termination of a call." Id.

126 See id. Although most of the examples given in the Third Report and Order are signals that would be audible to the subject, in-band and out-of-band signaling also includes nonaudible signals, such as remotely activated telephone message lights or text messages. See id. at para. 89. Signals that do not result in a message to the subscriber are not "call-identifying information." See id.

127 See id.

128 See id. at para. 95.

129 See id. (bringing a time stamp within range of the Section 102 definition of "call-identifying information" and noting its necessity in associating the call-identifying information with the underlying communication).

130 See id. at para. 96. Transmission to law enforcement must occur "within eight seconds 95% of the time." Id.

131 See id. at paras. 97, 101. Paragraph 97 of the Third Report and Order describes functions requested under the heading of "surveillance status" as including "the date, time
Apart from the fact that carriers do not currently generate this information, and it is entirely separate from any existing communications or signals that could be intercepted legally, the Commission concluded that surveillance status information was not itself "call-identifying information."132

7. Continuity Check Tone

A continuity check tone, as requested by the FBI, consists of a dial tone transmitted over a call content channel to a law enforcement agency whenever the wiretap subject's telecommunications medium (subject to the intercept order) is not in use.133 The Commission attempted to distinguish this tone from surveillance status information on the basis that a continuity check tone effectively only notifies carriers and law enforcement agencies when an active call occurs. However, it used essentially the same reasoning to exclude both features from the assistance capability mandates of CALEA.134

8. Feature Status

Feature status was the third punch list feature held to be outside the scope of CALEA's assistance capability mandates.135 The Commission defined feature status information as notification of certain modifications to the wiretap subject's calling service subscriptions.136 Although it noted that such information can be obtained from existing records by sending a subpoena to a carrier, the Commission determined that feature status messages were neither "call-identifying information" nor communications, and thus excluded these messages from the requirements of CALEA Section 103.137

9. Dialed Digit Extraction

The Commission wrestled with the versatile utility of digits dialed after an initial call connection (often referred to as "post-cut-through digits")138 in the Third Report and Order in an attempt to delineate the characteristics of digits comprising call content and those which merely route the call to its destination.139 At odds were the necessity of access to digits dialed after the initial connection to a long-distance carrier using a toll free access number, and the privacy interest in digits dialed for purposes of conducting a telephone banking transaction or using a credit card to order merchandise.140 The privacy issue was treated in the Third Report and Order as subordinate to the cost of developing technology capable of distinguishing the two types of post-cut-through digits. Thus, the Commission responded in a manner consistent with its disposition toward packet-mode communications and found that delivery of all post-cut-through digits is an assistance capability requirement of CALEA Section 103.141 The practical effect of this conclusion is that all post-cut-through digits will be accessible to law enforcement agencies conducting surveillance under the authority of a pen register order.142 As with packet-mode communications, the Third Report and Order appears to leave the privacy of post-cut-through digits (at least temporarily) in the hands of intercepting law enforcement agencies restrained only by a minimization requirement and the exclusionary rule.143

IV. ANALYSIS

The Commission's Third Report and Order conveys an intention to preserve the status quo for

132 See id. at para. 101.
133 See id. at para. 102.
134 See id. at paras. 102 n.197, 106 (contrasting the continuity check tone from surveillance status information and defining the relevant scope of the latter as whether the wiretap is operational).
135 See id. at para. 111.
136 See id. at para. 107. Examples include the addition or deletion of such service capabilities as call waiting and conference calling, as well as a change of telephone number or disconnection of service. See id.
137 See id. at para. 111.
138 Id. at para. 112.
139 See id. at para. 119–123.
140 See id. at para. 119. The Commission held that post-cut-through digits dialed for call-routing purposes were call-identifying information. See id. Other post-cut-through digits, such as credit card and bank account numbers, are considered call content and thus meritting additional constitutional protection. See id. at para. 114 (discussing comments of EFF, EPIC and ACLU). While the former is legally accessible under pen register authority, the latter, if treated as call content, should not be accessible. See id.
141 See id. at para. 123.
142 See id.
143 See id. See also discussion supra notes 9–10 (introducing Weeks and the exclusionary rule).
law enforcement while strictly construing the language of CALEA so as to minimize its economic impact on the telecommunications industry. Indeed, the Third Report and Order leaves intact the J-standard developed by industry participants. Assuming that developers of the J-standard had their own economic interests in mind, the cost to industry of implementing CALEA should be minimized. Of course, this is not to say that the unsubsidized cost of CALEA implementation will be small.144

Moreover, the additional technical capability requirements defined by the Third Report and Order were selected carefully to conform to existing J-standard features as closely as possible without depriving law enforcement agencies of traditionally available electronic surveillance capabilities.145 This view of the Commission's action compels the conclusion that it satisfied two of the three major policies behind CALEA. Those policies are: "(1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies."146 It was the Commission's supposed failure to refrain from effectively making "a broad range of private information"147 available to law enforcement surveillance that inspired the arguments against CALEA implementation made by industry and civil liberties groups in their consolidated appeal of the Third Report and Order.148

A. Petition for Review of the Third Report and Order

Following the FCC's adoption of the Third Report and Order in August 1999, two industry associations and three civil liberties groups filed petitions for review in the U.S. Court of Appeals for the District of Columbia Circuit.149 The Electronic Frontier Foundation ("EFF") filed a petition for review in the Ninth Circuit that was subsequently transferred to the D.C. Circuit.150 After

144 The high estimate of the total industry cost for implementation of the J-standard without any punch list features exceeds $4 billion. See Third Report and Order, 14 FCC Rcd. at para. 20 (referring to the Cellular Telecommunication Industry Association's estimate). Aggregate revenue estimates by five major telecommunications equipment manufacturers, on the other hand, total $916 million for the core J-standard and an additional $414 million for all nine punch list items. See id. at para. 30, app. B (breaking down manufacturers' cost estimates by punch list item and distinguishing between wireline and wireless service equipment). Of the total cost, Congress initially authorized $500 million for appropriation during fiscal years 1995 through 1998 to compensate certain qualifying carriers that comply with the assistance capability requirements. See 47 U.S.C. § 1009 (1994). Only $60 million was appropriated directly during that period. See Omnibus Consolidated Appropriations Act of 1997, Pub. L. No. 104-208, 110 Stat. 5009 (1996). This appropriation amount was primarily because of implementation delays. See 144 Cong. Rec. S12,852-02, S12,857 (daily ed. Oct. 21, 1998) (statement of Sen. Leahy). Congress has directly appropriated an additional $15 million for fiscal year 2000. See Consolidated Appropriations Act of 2000, Pub L. No. 106-113, 113 Stat. 1501, 1501A-4 (1999). There are essentially two ways that a carrier may qualify for compensation from the Attorney General for the carrier's CALEA compliance costs. One way, to qualify is by making necessary modifications "in connection with equipment, facilities, and services installed or deployed on or before January 1, 1995." 47 U.S.C. § 1008(a) (1994). The other way to qualify for compensation (concerning modifications to "equipment, facilities, and services installed or deployed after January 1, 1995") is for the carrier to 1) petition the Commission for a determination of whether compliance is "reasonably achievable" by the carrier, considering "whether compliance would impose significant difficulty or expense on the carrier or on the users of the carrier's systems"; and then 2) apply to the Attorney General for compensation, assuming a Commission determination that compliance is not reasonably achievable. Id. at § 1008(b).

145 See, e.g., discussion supra notes 103-106, 138-143 (discussing interception of packet-mode communications and post-cut-through digits). Rather than imposing prohibitive costs on the industry by requiring development of new surveillance technology usable only by law enforcement or depriving law enforcement of all access to communications previously available for three decades, the Commission split the difference and adopted the "readily available" technology. Also note the Commission's readiness to define "reasonably available" as available at the IAP. The inference here is that the Commission has done everything in its power to accommodate industry demands for the least expensive CALEA implementation possible.


147 USTA Brief, supra note 4, at 11.

148 See id. at 2 (noting that two of three issues presented for review focus on propriety of ordering overinclusive technical standards—that is, providing more information than previously available under wiretap authority); Brief of Petitioners Electronic Privacy Information Center ("EPIC"), Electronic Frontier Foundation ("EFF") and the American Civil Liberties Union ("ACLU") at 1, United States Telecom Ass'n v. FCC, (D.C. Cir. 2000) (Nos. 99-1442, 99-1466, 99-1475, 99-1525) (noting that three issues presented for review question FCC propriety of ordering overinclusive standards and the fourth questions whether the order directly violates the Fourth Amendment) (hereinafter EPIC Brief).

149 The industry groups are the USTA and CTIA. The civil liberties groups are EPIC, ACLU and CDT. See USTA Brief, supra note 4, at 2; EPIC Brief, supra note 148.

150 See EPIC Brief, supra note 148.
that denies law enforcement access to physical location information using trap-and-trace device authority. Yet allowing suspects to prevent effective disclosure of their locations merely by using mobile rather than wireline telephones cannot be what Congress intended when it sought to preserve law enforcement’s existing electronic surveillance capabilities. The Commission straddled the fence as best it could on this issue. First, it required that mobile telecommunications carriers develop the ability to provide cell site location. Second, the Commission held that such information could not be accessed by law enforcement under trap-and-trace device authority alone. In its role as “a forum . . . in the event a dispute arises over the technical requirements,” the Commission balanced three congressional purposes for enacting CALEA. Privacy protection, surveillance capability preservation and minimization of any hindrance to technological innovation received equal consideration. Despite petitioners’ arguments to the contrary, a different interpretation of “call-identifying information” with respect to cell site location would have compromised one or more of the driving forces behind CALEA’s enactment and would have taken the Commission beyond its authority as created under the Act.

In addition to physical location information, the petitioners also challenge the four punch list features dealing with post-connection dialing and signaling that the Commission adopted in the Third Report and Order. The petitioners’ chief argument that this capability preserves the electronic surveillance status quo. Because law enforcement generally has access to the location associated with a wireline telephone number, the Commission reasoned that providing the cell site location for mobile communication interception neither expands nor contracts existing electronic surveillance authority. Congress apparently envisioned this potential gray area when it added a provision to CALEA consolidating these initial petitions, three more industry groups and three telecommunications companies intervened in the action.

The main concern of the petitioners’ briefs is privacy protection. However, each argument turns on whether the Commission overstepped its authority, or acted in an arbitrary and capricious manner when it promulgated technical standards for CALEA implementation in the Third Report and Order. The first assistance capability challenging by petitioners is the Third Report and Order’s conclusion that cell location at the beginning and end of a wireless telephone call is “call-identifying information” and therefore must be made available to law enforcement. The petitioners put great emphasis on the danger that disclosing such information poses to individual privacy, characterizing the potential use of such information as physical location tracking. Despite a plausible construction of the statutory definition of “call-identifying information,” however, the petitioners fail to address the Commission’s argument that this capability preserves the electronic surveillance status quo. Because law enforcement generally has access to the location associated with a wireline telephone number, the Commission reasoned that providing the cell site location for mobile communication interception neither expands nor contracts existing electronic surveillance authority.

Congress apparently envisioned this potential gray area when it added a provision to CALEA § 1001 (2) as limited to telephone numbers only.

151 The intervening industry groups are the Personal Communications Industry Association (“PCIA”), the Rural Cellular Association (“RCA”) and the Telecommunications Industry Association (“TIA”). Companies intervening as of Jan. 20, 2000 (the filing date of the petitioners’ briefs) are AirTouch Communications, Inc., Sprint Spectrum, L.P. and U.S. West, Inc. See id. at iv. Note that many of the intervenors are concerned specifically with mobile telecommunications services.

152 See id. at 2; USTA Brief, supra note 4, at 11. Privacy protection concerns, as referenced in the accompanying text, include both Title III and Fourth Amendment violations. Many of the arguments made in both briefs use privacy concerns as bases for concluding that the Commission exceeded its authority under CALEA.

153 See USTA Brief, supra note 4, at 18; EPIC Brief, supra note 148, at 16.

154 See USTA Brief, supra note 4, at 21 (referring to cell location information as enabling “law enforcement officials to monitor a person’s location in near real-time”). Yet the Commission explicitly stated that it would require no such capability. See Third Report and Order, 14 FCC Rcd. at para. 46.

155 See USTA Brief, supra note 4, at 19–20 (construing the definition of “call-identifying information” in 47 U.S.C.

156 See Third Report and Order, 14 FCC Rcd. at para. 45. Law enforcement agencies have previously had access to the location of a wireline telephone either from their own 911 databases or from a telephone carrier’s records. See id.


159 See Third Report and Order, 14 FCC Rcd. at para. 44. Most mobile carriers apparently contemplated providing such information, as this capability is included in the J-standard. See id. at para. 45.


161 See USTA Brief, supra note 4, at 11. Petitioners argue that the Third Report and Order conflicts with the purpose of CALEA in this regard and offer little reasoning to support their conclusions. See id.

162 See id. at 22–27. These four contested punch list features are: dialed digit extraction; party hold, join and drop-on conference calls; subject-initiated dialing and signaling; and in-band and out-of-band signaling. See id.
concern is that some of this information can be considered call content and thus could be subject to Fourth Amendment privacy protections.\textsuperscript{165} This concern really applies only to dialed digit extraction. In fact, the petitioners’ only appropriate argument against mandating law enforcement access to the other contested punch list features seems to be that these features should not be considered “call-identifying information” within the meaning of CALEA.\textsuperscript{164}

It is unclear why this should be the case, notwithstanding the petitioners’ careful construction of the Act’s statutory language and legislative history in their briefs. Petitioners offer no compelling policy reason to support their implication that, in an age of versatile telecommunications services, law enforcement agencies acting under proper court-ordered wiretap authorization should not receive information necessary to match call-identifying information with call content.\textsuperscript{165} Even if the four challenged punch list items are not construed as call-identifying features, they would allow law enforcement agencies acting under pen register or trap-and-trace device authority to make sense of the telephone number information received during electronic surveillance. Suppose, for example, that an intercept subject hosts a conference call with multiple participants. At best, a pen register would capture only those digits dialed by the subject who set up the conference call. Meanwhile, a trap-and-trace device might capture the phone numbers of other parties joining the call or, at least, the phone number of the facility hosting the conference call. Without additional information provided by telecommunications carriers to law enforcement agencies, these numbers captured by electronic surveillance would be difficult or impossible to understand.\textsuperscript{166}

Compare this example to what was once the only possible situation facing law enforcement in electronic surveillance. One single telephone dialed a connection request to another single telephone, and the only numbers with any significance to the call were those dialed prior to connection.\textsuperscript{167} Law enforcement agencies gathered this information using pen registers or trap-and-trace devices for the express purpose of identifying “the associates and confederates of those believed to be conducting the illegal operation.”\textsuperscript{168} That identification often is no longer possible without the additional information contained in party hold, join and drop signals on conference calls; subject-initiated dialing and signaling; and in-band and out-of-band signaling. Thus the Commission had no real choice but to include this information within the scope of “call-identifying information” under CALEA. Otherwise, the Commission would have failed to preserve the status quo of electronic surveillance capability for law enforcement agencies acting under pen register or trap-and-trace device authority.\textsuperscript{169}

The petitioners make a stronger case against the adoption of dialed digit extraction as a technical requirement in the \textit{Third Report and Order}. While the other three punch list items contested by the petitioners cover information regarding changes in the status of an intercept subject’s communication or changes in the identities of other parties to the call, dialed digit extraction includes all numbers dialed after the initial call has been connected.\textsuperscript{170} The petitioners argue that requiring carriers to provide this information runs afoul of both the Fourth Amendment and Title III because the numbers dialed are often credit card numbers, bank account numbers or passwords, all of which are properly considered call content.\textsuperscript{171} They suggest that as “call-identifying information” pursuant to the \textit{Third Report and Order}, these numbers would have to be made availa-

\textsuperscript{165} \textit{See EPIC Brief, supra} note 148, at 11–12.
\textsuperscript{164} \textit{See USTA Brief, supra} note 4, at 24–27.
\textsuperscript{165} CALEA, in fact, requires that authorized access to call-identifying information should be provided by telecommunications carriers to law enforcement agencies “in a manner that allows it to be associated with the communication to which it pertains.” 47 U.S.C. § 1002(a)(2)(B).
\textsuperscript{167} \textit{See id. at 13 (“[U]ntil recently, the question of system design was never an issue for authorized surveillance”).}
\textsuperscript{168} \textit{New York Tel. Co., 434 U.S. at 162.}
\textsuperscript{169} \textit{See Third Report and Order, 14 FCC Rcd. at paras. 74, 82, 89 (finding party hold, join, and drop signals on conference calls; subject-initiated dialing and signaling information; and in-band and out-of-band signaling to be call-identifying information). These paragraphs also hold that the first two of the three items listed here are necessary for law enforcement agencies conducting electronic surveillance to know who is talking to whom. See id.}
\textsuperscript{170} \textit{See USTA Brief, supra} note 4, at 22.
\textsuperscript{171} \textit{See id.}
ble to law enforcement officers acting only under the authority of a pen register order.172

Digits dialed after the initial connection is made also include calls placed using a long-distance carrier that offers services accessible by a toll free number.173 The Commission found these numbers to be “call-identifying information.”174 The problem lies in the local carrier’s inability to distinguish telephone numbers from bank account numbers once the initial connection has been made.175 The local carrier’s expense of extracting post-cut-through digits is high enough without requiring detection and separation of two kinds of numbers before delivering them to law enforcement.176 Other alternatives considered by the Commission were either even more invasive of privacy than dialed digit extraction, or considered too time consuming or inefficient to be feasible.177 All things considered, the Commission determined that all interests would be served best by including dialed digit extraction in the technical capabilities required by CALEA.178 In light of the unfeasibility of the alternatives, this became an all-or-nothing standard. To exclude the dialed digit extraction capability entirely would contravene the primary mandate of CALEA, which is to preserve law enforcement’s ability to carry out properly authorized electronic surveillance in the face of rapidly changing telecommunications technology. Adopting this dialed digit extraction standard maintains familiar application of the minimization requirement to law enforcement wiretap applications, leaving individual privacy no worse off in the context of a legal wiretap than it has been since 1968.179

With respect to packet-mode communications, both the petitioners’ arguments and the Commission’s conclusions are analogous to those made regarding dialed digit extraction. It is another all-or-nothing situation where excluding the capability would be entirely against the driving purpose of CALEA but requiring distillation of specific information contained within packets would be prohibitively expensive—not to mention a potentially severe impediment to future industry innovation. Yet packet-mode communications rapidly are becoming ubiquitous telecommunications technology to be exempted from wiretapping beyond the short term.180 As with dialed digit extraction, the petitioners argue that the Third Report and Order gives law enforcement agencies more information about surveillance subjects than they are authorized to receive—that is, law enforcement receives information about call content under CALEA but needs only to obtain a warrant for “call-identifying information.”181 One difference from dialed digit extraction is that with packet-mode wiretaps, law enforcement officers likely will have complete access to voice communications and not just credit card or bank account numbers.182 A more significant difference (as the technology currently exists) is that, unlike post-cut-through digits in circuit-mode communications, packet-mode call content is essentially inseparable from “call-identifying information.”183

Because packet-mode communications by design make more efficient use of telecommunications networks than circuit-mode communications, any government-imposed redesign of the technology to facilitate separation of call-identifying information from content would violate CALEA’s policy against impeding new technologi-

172 See id.
173 See id.
175 See USTA Brief, supra note 4, at 23.
176 The Commission noted that digit extraction alone would be more expensive than any other punch list item. See Third Report and Order, 14 FCC Rcd. at para. 123.
177 One alternative consisted of law enforcement obtaining full wiretap authority in order to access all post-connection communications. Such authority is, of course, more difficult to obtain than that required for a pen register, effectively raising the standard of proof required for a pen register order. Another alternative contemplated directing a pen register order to each carrier with facilities used in a given communication by the intercept subject. Even if it was feasible, this alternative would likely result in numerous lengthy delays as law enforcement established multiple pen registers at multiple carriers that could easily change from call to call.
178 See id. at para. 120–22.
179 See id. at para. 123.
180 See discussion supra note 37–38(discussing the minimization requirement of Title III).
181 See USTA Brief, supra note 4, at 32.
182 See id. at 35 (stating that the Third Report and Order “permits law enforcement officials to intercept the contents of packet communications with nothing more than a pen register authorization”). See also Third Report and Order, 14 FCC Rcd. at para. 56.
183 See, e.g., Third Report and Order, 14 FCC Rcd. at para. 53 (noting the utter lack of feasibility of separating call content contained in individual packets from the accompanying call-identifying information).
The Commission readily admitted that it did not have enough information to make a final determination regarding technical standards for packet-mode surveillance assistance capabilities. For this reason, and in recognition of the increasing importance of packet-mode technologies, the Third Report and Order only established an interim requirement that carriers develop the ability to provide packet-mode communications in their entirety to properly authorized law enforcement agencies. It is expected that a permanent solution may be developed by the telecommunications industry (with the TIA leading the charge) as early as September 2000. Petitioners should also take comfort in the Commission’s footnote to the Third Report and Order that points out that many carriers have the ability to produce records containing only call-identifying information. Such capability would thus afford carriers the option of avoiding Fourth Amendment concerns entirely when confronted with a pen register order. Still, given the sheer number and variety of services already incorporating packet-mode technologies, in addition to the likelihood that they will continue to evolve and proliferate, privacy issues surrounding the interception of such communications are unlikely to disappear soon.

B. Why the Technical Standards of the Third Report and Order Should Stand

In the end, determining technical standards for CALEA implementation is fundamentally a matter of administrative policy rather than law and therefore appropriately within the province of the FCC. The petitioners’ claims of privacy concerns and complaints about FCC mandates that violate Title III and the Fourth Amendment are interlaced with pretext and clearly misplaced. Title III directly regulates electronic surveillance conducted by law enforcement, and not the activities of telecommunications carriers or the FCC. Furthermore, the Fourth Amendment creates individual rights against certain government searches and seizures but does not grant telecommunications carriers any rights to avoid FCC regulations. The Third Report and Order, in contrast, purports to govern neither the duties of law enforcement nor the enforcement authority of courts. It was intended, pursuant to Congress’ statutory command in CALEA, to update in technological terms a carrier’s legal duties under Title III, itself a long-time guide for courts applying Fourth Amendment warrant requirements to wiretaps. Exactly how this update, in an age of widespread technological change, could actually “mandat[e] unconstitutional searches and seizures” or violate both Title III and the Fourth Amendment is unclear. The Third Report and Order merely advocates the most efficient and effective application of CALEA’s solutions to recent law enforcement problems, while the petitioners’ proposals would allow federal wiretap law to be swept away on the current of market innovation and thus render CALEA toothless.

The Commission’s role under CALEA is to establish technical standards upon petition by a government agency or any other person who believes that any existing industry standards are deficient. Those technical standards, whether established by the Commission or within the telecommunications industry, constitute a safe harbor for compliance with the assistance capability responsibilities on telecommunications carriers or anyone else to assist law enforcement officials in effectuating wiretaps. Indeed, that was the primary impetus behind CALEA.

See id. at para. 55 (pointing out this potential danger).

See id.

See id.

See USTA Brief, supra note 4, at 54; EPIC Brief, supra note 148, at 9. Cf. Third Report and Order, 14 FCC Rcd. at para. 55 n.107. To the contrary, the USTA and EPIC Briefs misconstrue this statement by the Commission as “ignor[ing]” and “opt[ing] not to pursue this administratively and constitutionally sound alternative.”

See Third Report and Order, 14 FCC Rcd. at para. 51 (adopting AT&T’s comment that different packet-mode technologies may require different assistance capability standards).

requirements of the Act. As a safe harbor, compliance with those standards is not compulsory but merely suggested as a means of obtaining voluntary industry compliance with CALEA. For these reasons, the Third Report and Order does not actually mandate or require compliance with any of the technical standards defined therein. Even if it did somehow carry the weight of a legal mandate, such technological guidelines cannot dictate the level of proof binding on courts when confronted with an application by law enforcement for a wiretap order. The legal determination of the level of proof can only be made by courts themselves, acting pursuant to Title III, the federal pen register statute or the Fourth Amendment. In the event that the order sought does not exactly fit within the contemplated scope of these laws, Title III and Fourth Amendment case law provide factual scenarios to guide courts in determining the appropriate level of proof. Therefore, regardless of its language, the Third Report and Order has no actual authority to define the specific levels of proof necessary for certain types of surveillance.

Because the Commission neither intends to, nor actually does, redefine types of surveillance that may occur under existing legal authority, the petitioners’ arguments that the Commission exceeded CALEA, and violated Title III and the Fourth Amendment are based on a false premise. With the exception of the civil liberties groups that joined the appeal, the petitioners’ privacy arguments largely seem to be pretext for economic concerns about the costs of meeting technical standards in the Third Report and Order. Not only could compliance raise industry costs enough to affect subscription rates, but a widespread public perception that the new technical standards inherently lessen the privacy and security of telecommunications networks could conceivably cause subscribers to lose confidence in newer services and technologies. Any resulting loss of subscribers could then theoretically reduce the expected return on telecommunications carriers’ investment in developing new services and technologies and thus have the potential effect of chilling technological innovation. Yet one way or another, whether through higher taxes or increased telecommunications service rates, subscribers will end up paying for CALEA. Industry investments made today ultimately will cost less than future, forced upgrades and penalties imposed by regulatory or judicial action to ensure belated industry compliance with the Act. Otherwise, the fact that new technologies so challenged the traditional functionality of authorized wiretaps as to prompt CALEA’s enactment should reassure the true privacy advocates, because there remain a number of available technologies unaffected by the Act.

Regardless of the petitioners’ motivations to challenge CALEA and the Commission’s implementation duties under the Act, the courts will eventually have to address legal questions prompted by the development of new wiretap technologies. Only then should Title III and Fourth Amendment concerns come into play. For example, the Commission clearly foresaw the possibility that law enforcement will seek only pen register or trap-and-trace authority to intercept

\[199\] See, e.g., United States v. Escobar-de Jesus, 187 F.3d 148, 171 (1st Cir. 1999).

To the extent that Title III is designed to protect privacy interests similar to those reflected in the Fourth Amendment... that statutory purpose was served by the district court’s finding of probable cause to intercept and by the order’s inclusion of other items of particularity, including the identity of the person whose communications were to be intercepted, the nature and location of the telephone line to be intercepted, a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which the communications relate.

\[200\] See, e.g., id.
\[201\] See discussion supra note 144 (discussing various estimates of the cost of implementation).
\[202\] See America Rides the Wireless Wave, THE ECONOMIST, Apr. 29, 2000, at 57. This is pure speculation. As a whole, the general public appears to be oblivious to telephone privacy issues and to have gained rather than lost confidence in wireless services. A graph appearing in a recent issue of THE ECONOMIST shows mobile phone ownership penetration of all United States households in 1999 at over 30%. The level exceeded sixty percent in some urban areas.

\[203\] Two major examples of exempt technologies and services are encrypted or scrambled telecommunications, and any communication classified as “information services,” such as electronic mail or paging services. See 47 U.S.C. § 1002(b)(2)–(3); 47 U.S.C. § 1001(6) (defining “information services” for purposes of CALEA).
packet-mode communications.

However, there is no legal authority for such an order. Under the pen register statute, a court may issue an order "authorizing the installation and use of a pen register or a [trap-and-trace] device." A pen register is defined later in the statute as a device attached to a telephone line that identifies the telephone numbers dialed.

Furthermore, a trap-and-trace device is defined as identifying the originating telephone number of an incoming call.

With the governing statute expressly limited in scope to capturing telephone numbers, courts cannot issue pen register warrants authorizing the interception of packet-mode communications.

Thus the practical solution to this new problem is properly left either for the judicial system or Congress to remedy at a future date. The FCC has fulfilled its statutory duty and only a change in the statute or in Fourth Amendment doctrine will drastically alter the Third Report and Order now.

Just as technological advances prompted CALEA’s enactment, so too will they require continually updated technical standards for compliance with the Act’s assistance capability requirements that are designed to conform to the inherent limitations of the regulated technologies. CALEA does indeed regulate technology by requiring that certain capabilities be built into law enforcement assistance capabilities. In doing so, however, the statute does not attempt to limit the state of the art but aims merely to keep up with it. It is certainly not desirable in a free market society for the future of technological innovation to be threatened by future technological change.

Instead, there must be compromises enabling technology and the law to evolve together. Thus Congress conceived the underlying design of CALEA—to provide advance notice to the telecommunications industry of the types of law enforcement assistance functionality that it will be required to build into its new service offerings to the public.

There are effectively three parties upon whom the assistance capability provisions of CALEA impose duties: the telecommunications industry, law enforcement agencies and the FCC. The industry had the initial responsibility for developing technical standards that met the Act’s statutory requirements. Law enforcement agencies were handed the task of identifying problems, both with existing technology and the technical standards proposed by industry for CALEA compliance. Finally, in the event of a dispute over implementation between law enforcement agencies and the telecommunications industry, the FCC was chosen as the referee. The telecommunications industry understandably wanted to minimize the cost of implementation and thus proposed standards that required as few changes as possible to existing facilities. Law enforcement agencies, of course, hoped to take advantage of the benefits of technology, both to overcome technical surveillance difficulties that they faced with newer telecommunications services and to expand their overall electronic surveillance capabilities.

Armed with telecommunications expertise but having scant experience with the law governing searches and seizures, the FCC was thrust into the unfortunate position of balancing these often competing interests as directed by the statute. At the same time, it had to provide telecommunications industry participants clear notice of exactly what would be required of them in terms specific enough to ensure their compliance. This is precisely what the Commission did—as best it could given the limitations of both the law and the existing technology—because Congress had decided that “somebody” had to do it. If anything, more deference should be given to the wiretap laws in

---

204 See Third Report and Order, 14 FCC Rcd. at para. 56.
208 See discussion supra Part III.C (discussing the Third Report and Order’s treatment of the FBI Punch List items). Despite any implications of the Third Report and Order to the contrary, there is no provision in CALEA that equates “call-identifying information” with information accessible pursuant to a pen register order. Given the Commission’s inclusion of such punch list items as party hold, join and drop on conference calls, and in-band and out-of-band signaling within the

---

209 For an in-depth discussion of the operability of the “law of cyberspace” as a teacher of narrow tailoring in regulatory design and other issues presented by the interplay between law and technology, see Lawrence Lessig, The Law of the Horse: What Cyberlaw Might Teach, 113 Harv. L. Rev. 501 (1999).
210 Thus the FBI must define standards in addition to those minimally adopted by industry or risk having its wiretap authority preempted by changes in technology.
analyzing these issues than to technology in recognition of the exponentially longer amount of time that it has traditionally taken for the law to change. Technology, by nature, has always had the advantage in the arena of privacy creation—if not by design then by virtue of its mystery.211

The Third Report and Order should stand because it does not directly violate any constitutional rights. The report’s five-year gestation period, complete with ample industry participation, should quash any notions that the Commission acted arbitrarily or capriciously. It implements a remarkable (if imperfect) attempt at harmonizing the accelerating evolution of law and technology in the wiretap context. While it should be expected that, over time, certain standards will need refinement, short-term competitive barriers to implementation have dropped significantly. In a single stroke, the FCC provided the telecommunications industry with the external impetus necessary for CALEA implementation that was previously lacking and trivialized the industry’s earlier fears that action not taken by the entire industry might competitively disadvantage the individual actor. Congress used the Commission’s rulemaking authority as a check to balance the competing interests of progress and public safety, each represented on behalf of the general public by the telecommunications industry and law enforcement. The Commission should not relinquish this hard won anchor point for the implementation of CALEA, lest the growing rift between telecommunications technology and the law become impassable.

V. CONCLUSION

The technical standards contained in the FCC’s Third Report and Order, In Re the Communications Assistance for Law Enforcement Act (“CALEA”), begin to effectively implement the assistance capability requirements of the Act as envisioned by Congress. The Commission’s proper exercise of its rulemaking authority under CALEA should overcome the telecommunications industry’s reluctance to comply with all law enforcement requests for additional features in electronic surveillance. This result was warranted by statutory design without contravention of either Title III or the Fourth Amendment, because the capability standards constitute a safe harbor for compliance with the Act and not a determination of the appropriate level of proof required for authorization of certain types of electronic surveillance. Although the Third Report and Order highlights questions for courts regarding such requirements for the legal authorization of certain new types of interceptions, the preservation of CALEA’s integrity demands that these issues must be viewed as a result not of the Commission’s rulemaking but of the limitations inherent in some new telecommunications technologies.

For all of the above reasons, the Third Report and Order should be upheld. Collaterally, telecommunications carriers should embrace (sooner rather than later) upgrades to their facilities that bring them into compliance with CALEA’s new technical standards in order to avoid penalties and the potentially high cost of independently marketed upgrade packages. Congress, federal law enforcement agencies and the FCC all have responded to the lack of industry initiative that compelled enactment of CALEA. The government has now mandated the incorporation of specific capabilities for making effective, legal wiretaps into the designs of current and future telecommunications technology and services. Industry participants should welcome this opportunity to maintain proprietary control over both the enabling and the limitation of wiretap capabilities in their own facilities. From a forward-looking economic perspective, such control appears preferable either to forcing telecommunications carriers to pay for piecemeal upgrades in the event of future wiretap orders or to having the government dictate new detailed technical capability standards every time telecommunications technology takes another step forward.

211 As noted above, CALEA would not have been necessary were it not for the de facto privacy created by the increasingly numerous, complicated and cryptic electronic signals that now comprise telecommunications.