Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of:	)	
Communications Assistance for Law Enforcement Act	)	CC Docket No. 97-213

REMAND COMMENTS OF DEPARTMENT OF JUSTICE AND FEDERAL BUREAU OF INVESTIGATION

Louis J. Freeh, Director
Federal Bureau of Investigation

Larry R. Parkinson
General Counsel
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

Honorable Janet Reno
Attorney General of the United States

William B. Schultz
Deputy Assistant Attorney General

Douglas N. Letter
Appellate Litigation Counsel
Civil Division
U.S. Department of Justice
601 D Street, N.W., Room 9106
Washington, D.C. 20530
(202) 514-3602

TABLE OF CONTENTS

SUMMARY

In August 1999, the Commission modified a technical standard (the J-Standard) adopted by the telecommunications industry as a "safe harbor" for wireline, cellular, and broadband PCS carriers who are subject to the assistance capability requirements of CALEA. Acting pursuant to Section 107(b) of CALEA, the Commission determined that the J-Standard omitted important assistance capabilities that are required by CALEA. The Commission therefore ordered that the J-Standard be modified to include six missing "punch list" capabilities.

The D.C. Circuit has vacated the Commission's decision with respect to four of the six punch list capabilities and has remanded for further proceedings regarding those capabilities. The Court of Appeals did not hold that the vacated capabilities are legally inappropriate or unwarranted under Section 107(b). Instead, the Court of Appeals held that the Commission had not adequately explained its grounds for adding the capabilities.

As we show below, the Commission was fully justified in its original conclusions regarding the punch list items, and the Commission can readily provide the reasoned explanation for those conclusions that the Court of Appeals has called for. First, all of the information covered by the punch list capabilities constitutes "call-identifying information," and the loss of this information would represent a serious reduction in the surveillance capabilities that law enforcement traditionally has had in the POTS environment – a result that Congress manifestly meant to foreclose. Second, adding the punch list capabilities to the J-Standard is fully consistent with the cost criteria of Section 107(b) – a conclusion is

reinforced by new cost information that was not available to the Commission at the time of its original decision. Third, all of the punch list capabilities, including dialed digit extraction, satisfy the privacy concerns of Section 107(b). The Commission therefore should reinstate the vacated punch list capabilities and provide a complete explanation of the grounds for its decision, thereby meeting the D.C. Circuit's objections to the Commission's original decision.

DISCUSSION

On October 17, 2000, the Commission issued a Public Notice in response to the recent decision of the D.C. Circuit in USTA v. FCC, 227 F.3d 450 (2000). The D.C. Circuit's decision in USTA vacates a portion of the Commission's Third Report and Order in this proceeding and remands for further consideration by the Commission. The Public Notice invites comments on issues raised by the D.C. Circuit's decision. The Department of Justice and the FBI (jointly "the government") submit these comments in response to the Public Notice.

1. This proceeding originated in March 1998, when the government and several other parties petitioned the Commission under Section 107(b) of the Communications Assistance for Law Enforcement Act ("CALEA"), 47 U.S.C. § 1006(b). Section 107(b) provides for the Commission to review industry "safe harbor" technical standards (see 47 U.S.C. § 1006(a)) in order to determine whether they are "deficient" – that is, whether they fall short of satisfying the assistance capability requirements set forth in Section 103 of CALEA, 47 U.S.C. § 1002. If the Commission determines that an industry standard is deficient, Section 107(b) requires the Commission to "establish, by rule, technical requirements or standards that * * * meet the assistance capability requirements" of Section 103. 47 U.S.C. § 1006(b)(1). In framing technical standards that "meet the assistance requirements" of Section 103, the Commission must consider several specific statutory criteria. Id. § 1006(b)(1)-(5). Among other things, Section 107(b) directs the Commission to adopt standards that "meet the assistance capability requirements * * * by cost-effective methods";

"protect the privacy and security of communications not authorized to be intercepted"; and "minimize the cost of such compliance [with the assistance capability requirements] on residential ratepayers." Id. § 1006(b)(1), (2), (3).

The government asked the Commission to modify J-STD-025 ("J-Standard"), a safe-harbor standard adopted in December 1997 for voluntary use by wireline and wireless telecommunications carriers in meeting the assistance capability requirements of Section 103. The government identified nine capabilities, collectively referred to as the "punch list," which were omitted from the J-Standard but which the government regarded to be required by Section 103. The other parties asked the Commission to eliminate the J-Standard's provisions regarding delivery of wireless terminal location information and to modify the J-Standard's provisions regarding delivery of packet-mode routing information.

On August 29, 1999, the Commission issued its Third Report and Order in this proceeding. The Third Report and Order concluded that the J-Standard was deficient with respect to six of the nine punch list capabilities, and directed industry to modify the J-Standard to add those capabilities. The Commission declined to modify the J-Standard's provisions regarding wireless location information and packet-mode information, although the Commission called on the Telecommunications Industry Association ("TIA") to prepare a technical report on the packet-mode issues.

Petitions for review of the Third Report and Order were filed in the D.C. Circuit pursuant to the Hobbs Act, 28 U.S.C. §§ 2341-2351. The petitioning parties challenged the Commission's decision with respect to four of the six punch list capabilities. The four

challenged punch list capabilities were: (1) dialed digit extraction; (2) subject-initiated dialing and signaling information; (3) in-band and out-of-band signaling; and (4) party hold/join/drop information. The petitioners also challenged the Commission's decision not to modify the J-Standard's wireless location information and packet-mode provisions.

On August 15, 2000, the D.C. Circuit issued a decision that granted in part and denied in part the petitions for review. The Court of Appeals denied the petitions with respect to the Commission's disposition of the wireless location information and packet-mode issues. 227 F.3d at 463-466. The Court of Appeals granted the petitions with respect to the Commission's disposition of the four contested punch list capabilities. Id. at 460-463. With respect to those capabilities, the Court of Appeals vacated the Third Report and Order and remanded the case to the Commission for further proceedings.

In vacating the Commission's decision regarding the four punch list capabilities, the Court of Appeals did not conclude that the decision was inconsistent with the terms of CALEA. See 227 F.3d at 460. Instead, the Court concluded that the Commission had failed to provide an adequate explanation of its reasons for adding the punch list capabilities to the J-Standard. First, the Court found that the Commission had not adequately explained why the information covered by the four punch list items constitutes "call-identifying information," as that term is defined in Section 102 of CALEA, nor had the Commission explained why the definition of "call-identifying information" in the J-Standard itself was deficient. Id. at 460-461. Second, the Court found that the Commission had not adequately explained how the punch list capabilities satisfy the cost criteria of Section 107(b)(1) and

Section 107(b)(3). Id. at 461-462. Third, the Court found that the Commission had not adequately explained how dialed digit extraction satisfies the privacy criterion of Section 107(b)(2). Id. at 462-463. The Court called on the Commission to provide a more complete explanation of the basis for its decision in each of these regards.

The Public Notice invites comments on the issues raised by the D.C. Circuit's remand order and on what actions the Commission should take to address the D.C. Circuit's concerns. The Public Notice specifically requests comments on the following matters:

> [1] [W]e seek comment on the definition of the term "call identifying information" as used in CALEA, discussed in the legislative history, and used in the interim standard, and whether the four punch list capabilities are covered by that term. Parties should address whether the four punch list capabilities are call identifying information, whether deficiencies exist in the interim standard, and how each of the four punch list capabilities would address such deficiencies.
>
> [2] We also seek comment on the definition of the term "cost-effective methods," how cost effectiveness should be measured in relation to the four punch list capabilities, the implementing costs for the punch list capabilities, and how requiring these capabilities would affect residential ratepayers. Commenters should provide information on alternative methods for providing the four capabilities, and for each alternative method provide specific information on implementing cost and the effect on residential ratepayers. Commenters should suggest ways for carriers to minimize costs to residential ratepayers.
>
> [3] Finally, commenters should provide information on how the four capabilities, in particular post-cut-through dialed digit extraction, could be implemented while satisfying CALEA's requirement to "protect the privacy and security of communications not authorized to be intercepted."

2. The government submits the following comments in response to the Commission's Public Notice. The comments are divided into four parts.

Part I (pp. 9-29 infra) addresses whether the kinds of information covered by the four punch list capabilities constitute "call-identifying information." As we show, the statutory definition of "call-identifying information" is properly construed to reach the information provided by each of the contested capabilities. To the extent that the J-Standard's definition of "call-identifying information" and its constituent terms does not extend to this information, it is inconsistent with CALEA itself and must be rejected as deficient by the Commission.

Part II (pp. 29-46 infra) addresses the cost issues raised by the Court of Appeals. We show that the aggregate cost of implementing the J-Standard and the punch list capabilities is modest; the incremental cost of implementing the four contested punch list capabilities is negligible; and there are no alternative methods of curing the deficiencies in the J-Standard that are more cost-effective than the punch list capabilities. For these reasons, adding the punch list capabilities to the J-Standard is fully consistent with the cost criteria of Section 107(b).

Part III (pp. 46-57 infra) addresses the privacy issues identified by the Court of Appeals. The only punch list capability with respect to which the Court of Appeals raised privacy questions is dialed digit extraction – the capability of an originating carrier to extract "post-cut-through" dialed digits from a call content channel and deliver them to law enforcement. We show that requiring carriers to be capable of performing dialed digit extraction does not conflict with the privacy provisions of Section 103(a) and Section 107(b) of CALEA.

Finally, Part IV (pp. 57-60 infra) identifies several relatively minor respects in which the Commission should modify the original rule to clarify its scope and operation. For example, we recommend that the rule be modified to make clear that the Commission is only addressing what information a carrier must be capable of delivering to law enforcement, and is not purporting to compel the actual delivery of any information in the absence of appropriate legal authorization.

Apart from the modifications discussed in Part IV, the Commission should reinstate its original rule as set forth in the Third Report and Order. All that is required to support the vacated provisions of the original rule is for the Commission to provide the kind of reasoned explanation that the D.C. Circuit found to be lacking in the Third Report and Order. As demonstrated in Parts I through III of these comments, reasoned explanations are readily at hand.

The government has previously filed comments relating to CALEA's assistance capability requirements in response to the Commission's original Public Notice (released in April 1998), and the Commission's Further Notice of Proposed Rulemaking (released in November 1998). See DOJ/FBI Comments Regarding Standards for Assistance Capability Requirements, CC Docket No. 97-213 (filed May 20, 1998) ("First Government Comments"); DOJ/FBI Reply Comments Regarding Standards for Assistance Capability Requirements, CC Docket No. 97-213 (filed June 12, 1998) ("First Government Reply Comments"); DOJ/FBI Comments Regarding Further Notice of Proposed Rulemaking (filed December 14, 1998) ("Second Government Comments"); DOJ/FBI Reply Comments

Regarding Further Notice of Proposed Rulemaking (filed January 27, 1999) ("Second Government Reply Comments"). We renew those comments and incorporate them here by reference.

I. The Types of Information Covered by the Punch List Capabilities Constitute "Call-Identifying Information"

Section 103(a)(2) of CALEA requires every telecommunications carrier to be capable of expeditiously isolating and enabling the government to access reasonably available "call-identifying information," pursuant to a court order or other lawful authorization. 47 U.S.C. § 1002(a)(2). "Call-identifying information" is defined by CALEA to mean "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier." Id. § 1001(2).

In the Third Report and Order, the Commission determined that the information covered by the four now-vacated punch list capabilities constituted "call-identifying information" within the meaning of that term in CALEA. The D.C. Circuit held that the Commission had not adequately explained the basis for that determination. As we now show, the Commission had ample grounds for determining that CALEA's definition of "call-identifying information" encompasses the information provided by the four punch list capabilities.

A. General Considerations

The Court of Appeals concluded that CALEA's definition of "call-identifying information" neither clearly excludes nor clearly includes the information covered by the contested punch list capabilities. See 227 F.3d at 457-459. As a result, the Court of Appeals regarded this as a "Chevron step two" case – a case in which Congress has assigned the agency the task of filling gaps and resolving ambiguities in the statutory scheme through the agency's interpretation and application of the statute's terms. See Chevron U.S.A., Inc. v. Natural Resources Defense Council, 467 U.S. 837, 843-845, 865-866 (1984). Under Chevron step two, the agency's resolution of these issues is entitled to deference as long as it is based on a "permissible construction of the statute." Id. at 843. In carrying out its own interpretive responsibilities under Chevron, the Commission should adhere to the following principles.

1. As a threshold matter, the Commission should adopt a presumption that "call-identifying information" includes information that law enforcement has traditionally been able to receive through authorized electronic surveillance in the POTS environment – in particular, information that has been available when law enforcement conducts pen register and trap-and-trace surveillance. Although the parties to this proceeding have argued vigorously over whether CALEA was intended to provide law enforcement with more information than it historically received in the POTS environment, it is undisputed that, at the very least, CALEA was intended to ensure that law enforcement does not receive less information than it did in the POTS environment. See, e.g., H. Rep. No. 103-827, 103d Cong., 2d Sess. 9 (1994), reprinted in 1994 USCCAN 3489 ("The purpose of [CALEA] is

to preserve law enforcement's ability * * * to intercept communications"); id. at 16, reprinted in 1994 USCCAN at 3496 (CALEA "requires telecommunications common carriers to ensure that new technologies and services do not hinder law enforcement access to the communications of a subscriber"). As a result, the Commission should begin with the presumption that CALEA's definition of "call-identifying information" maintains law enforcement's "access to information [that] it had in the past." Id. at 22, reprinted in 1994 USCCAN at 3502.

We do not mean to suggest that this presumption should be an irrebuttable one. If the language or legislative history of CALEA plainly forecloses treating particular information as "call-identifying information," then the fact that the information has historically been available to law enforcement would not be sufficient to carry the day. Conversely, if the language or legislative history of CALEA affirmatively compels treating particular information as "call-identifying information," the fact that the information has not traditionally been available to law enforcement would not be dispositive. But where CALEA's language and legislative history neither compel or foreclose treating particular information as "call-identifying information," the traditional availability of the information to law enforcement should be given substantial weight.

In our earlier filings, we submitted declarations that summarize how pen register surveillance is carried out in the POTS environment and what kinds of information have historically been available. Traditional pen register surveillance involves establishing a direct physical connection to the "local loop," the line that runs between the subject's phone

and the carrier's central office. See Second Government Reply Comments, Yarbrough Declaration ¶ 6; Second Government Reply Comments, Cutright Declaration ¶ 4. The surveillance equipment detects the electrical impulses transmitted over the local loop and retransmits them to a collection site. In the POTS environment, phone numbers and other dialing and signaling activity often are transmitted "in-band" over the same circuit as the voice communication. See Yarbrough Dec. ¶ 29; Cutright Dec. ¶ 6. As a result, the electrical impulses transmitted to law enforcement include not only the intercept subject's dialing and signaling activity, but also the audio portion of the call. The transmitted signals are processed by equipment that strips out the audio signals, then decodes and records the signals used in call processing. This includes not only the phone numbers dialed by the subject, but also all signals that are sent from the intercept subject to the carrier, such as "off-hook" and "on-hook" signals and hook flashes, all signals that are transmitted from the carrier to the intercept subject, such as ringing tones, busy signals, and similar signaling information. See Yarbrough Dec. ¶¶ 6-7. It is imperative for the Commission to keep this traditional model in mind when addressing the applicability of CALEA to the contested punch list capabilities.

2. The Commission should also give careful attention to the constituent parts of Section 102(2)'s definition of "call-identifying information." As noted, "call-identifying information" includes "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber * * * ." 47 U.S.C. § 1001(2) (emphasis added). The Commission should consider each of

the underscored terms in this definition: "dialing and signaling information"; "identifies"; "origin, direction, destination, or termination"; and "each communication."

· **"dialing or signaling information"**

From the outset of this proceeding, other commenters have argued that only telephone numbers constitute "call-identifying information." The Commission rejected that argument in its original decision, and it should reiterate its original conclusion that "call-identifying information" is not confined to telephone numbers. We have addressed this issue at length in our prior filings, and rather than repeat that discussion here, we invite the Commission to review our earlier comments. See, e.g., Government Reply Comments at 31-34. We also urge the Commission to review the D.C. Circuit's discussion of this issue, which identifies a number of shortcomings with the argument that only phone numbers constitute "call-identifying information." See USTA v. FCC, 227 F.3d at 458-459. The Commission should state explicitly that "call-identifying information" includes all "dialing and signaling information" that identifies the origin, direction, destination, or termination of communications, not just telephone numbers, and should set forth the reasons supporting that conclusion.

· **"identifies"**

With respect to "identifies," it is important to remember that things can be "identified" in more than one way and by more than one kind of information. For example, an individual may be identified by name, age, race, sex, height, weight, and other identifying criteria. If a statute provided for the disclosure or withholding of "information that identifies an

individual," it would at least presumptively encompass all of these kinds of information. See, e.g., 18 U.S.C. §§ 2721(a), 2725(3) (Driver's Privacy Protection Act) (prohibiting state motor vehicle departments from disclosing "information that identifies an individual," including but not limited to the individual's "photograph, social security number, driver identification number, name, address * * * , telephone number, and medical or disability information"). So too here: the origin, destination, direction, or termination of a communication may be identified by more than one kind of dialing or signaling information. The Commission reasonably may construe "call-identifying information" to reach all such information.

· **"origin, direction, destination, or termination"**

Section 102(2) does not explicitly define "origin," "direction," "destination," or "termination." However, guidance regarding the meaning of three of these four terms can be derived from Section 103(a), the provision that sets forth CALEA's assistance capability requirements.

Section 103(a) requires telecommunications carriers to meet CALEA's assistance capability requirements with respect to their "equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications * * * ." 47 U.S.C. § 1002(a) (emphasis added). The underscored terms directly parallel "origination," "termination," and "direction" in Section 102(2). It therefore is reasonable to interpret "origination," "termination," and "direction" in Section 102(2) consistently with the way in which their counterparts are used in Section 103(a), particularly since Section 103(a)

is the principal part of CALEA that relies on Section 102(2)'s definition of "call-identifying information."

A party "originates" a communication when the party uses a carrier's equipment, facilities, or services to send (or attempt to send) a communication to another party. For example, a party who places an outgoing telephone call is originating a communication. Conversely, a party "terminates" a communication when the party uses a carrier's equipment, facilities, or services to receive (or attempt to receive) an incoming communication from another party. Thus, "originate" and "terminate" are complementary concepts that describe the same communication from two different perspectives -- that of the calling or sending party and that of the called or receiving party. The equipment, facilities, or services associated with the calling or sending party originate the communication and the equipment, facilities, or services associated with the called or receiving party terminate the communication. Finally, a party "directs" a communication when he uses equipment, facilities, or services to control the path or course of the communication. For example, if a party transfers an incoming call, he is thereby "directing" the communication.

When CALEA's definition of "call-identifying information" is viewed in this context, the meaning of "origin," "termination," and "direction" become easier to discern. "Dialing or signaling information that identifies the origin * * * of each communication" means information that identifies the use of equipment, facilities, or services to originate (transmit) a communication. "Dialing or signaling information that identifies the * * * termination of each communication" means information that identifies the use of equipment, facilities, or

services to terminate (receive) a communication. And "dialing or signaling information that identifies the * * * direction * * * of each communication" means information that identifies the use of equipment, facilities, or services to control the path or course of the communication.

The remaining term in Section 102(2), "destination," has no counterpart in Section 103(a). In common usage, the destination of something is its intended end point. See, e.g., Oxford English Dictionary 258 (1971 ed.) ("the place for which a person or thing is destined; the intended end of a journey or course"). Therefore, "dialing or signaling information that identifies the * * * destination * * * of a communication" is reasonably understood as information that identifies the equipment, facilities, and services toward which the communication is directed. In the context of a simple telephone call from party A to party B, this information will overlap with information that identifies the "termination" of the communication, since the facilities toward which the communication is directed by the calling party will be the same as the facilities that are used to terminate the communication. However, in more complicated calling scenarios, such as those involving call redirection, the destination of the communication and the termination of the communication will involve different equipment, facilities, and services, and different information will therefore identify the destination and the termination of the communication.

· **"each communication"**

Section 102(2) provides that "call-identifying information" includes all dialing and signaling information that identifies the origin, direction, destination, and termination of

"each communication generated or received by a subscriber * * * ." The Commission should note that a single call – in particular, a multi-leg call involving more than two parties – often will involve more than one "communication." For example, when a subject who is participating in a three-party conference call uses a feature key to toggle back and forth between the two legs of the call, speaking first to one of the parties and then to the other one, the subject is engaging in two separate communications, not one. Cf. 18 U.S.C. § 2510(1), (12) (definitions of "wire communication" and "electronic communication"). CALEA's definition of "call-identifying information" includes all dialing and signaling information that identifies the origin, direction, destination, and termination of each of these communications.

3. Finally, while the D.C. Circuit's decision calls on the Commission to explain how it has construed and applied "call-identifying information" and its constituent terms, the Commission is under no obligation to announce an all-encompassing definition of "call-identifying information" that goes beyond the confines of this proceeding to address and resolve all potential applications of the statutory terms. Instead, the Commission is free to construe "call-identifying information" with reference to the specific capabilities now at issue, leaving questions about the scope of the term in other contexts to be resolved in the future, if and when they arise. See, e.g., SEC v. Chenery Corp., 332 U.S. 194, 203 (1947) ("There is * * * a very definite place [in agency practice] for the case-by-case evolution of statutory standards"); CBS, Inc. v. FCC, 629 F.2d 1, 14-15 (D.C. Cir. 1980) (sustaining Commission's practice of construing provision of Communications Act of 1934 "on a case by case basis" rather than through "general interpretive statements"); cf. Cardoza-Foseca, 480

U.S. 421, 448 (1987) (in some cases, ambiguous statutory language "can only be given concrete meaning through case-by-case adjudication"). Nothing in the D.C. Circuit's decision is to the contrary.

B. Dialed Digit Extraction

Dialed digit extraction is a capability that permits a law enforcement agency to receive, on a call data channel, digits dialed by a subject when a call is connected to another carrier's service for processing and routing. See Third Report and Order ¶ 112. This capability is directed at "post-cut-through dialing" – digits that are dialed by an intercept subject, after his call has been "cut through" by the originating carrier, in order to reach the party with whom he wishes to speak. For example, if a subject dials "1-800-CALL-ATT" and is connected by the originating carrier to AT&T's long-distance calling-card service, then dials "202-555-1234" to reach an associate, the latter numbers are post-cut-through dialed digits. Under the Third Report and Order, the originating carrier must be capable of extracting those digits from the call content channel and delivering them to law enforcement on a call data channel.

In terms of its importance to law enforcement, dialed digit extraction is by far the most important of the four punch list capabilities vacated by the Court of Appeals. If law enforcement agencies are unable to obtain access to post-cut-through telephone numbers, the effectiveness of pen register surveillance will be gravely compromised, since an intercept subject will be able to conceal the numbers that he is calling by the simple expedient of using a calling-card service. This problem is particularly grave with regard to wireless phones, for

which there is no hard-wired "local loop" that law enforcement can use to monitor outgoing dialing activity. As wireless phone usage expands, law enforcement's ability to engage in pen register surveillance will correspondingly dwindle unless post-cut-through dialing can be obtained through dialed digit extraction.

In its prior comments, the government has explained why the definition of "call-identifying information" encompasses post-cut-through digits that are dialed for call routing purposes. See Government Reply Comments at 38-41; Second Government Comments at 66-67; Second Government Reply Comments at 23-26, 57-58. Simply stated, post-cut-through digits that are dialed for call routing purposes are "dialing * * * information" that "identifies" the "destination" and/or "termination" of the "communication generated" by the calling party. 47 U.S.C. § 1001(2). In terms of the statutory definition, a telephone number that is dialed "post-cut-through" is identical to a telephone number that is dialed "pre-cut-through." Indeed, one may readily imagine a subject dialing the same number to reach the same party on two different occasions – the first time by calling the party directly and the second time by dialing the same number after being "cut through" to a calling-card service. There is no possible statutory basis for suggesting that the same telephone number is "call-identifying information" the first time and something else the second time.

In previous stages of this proceeding, commenters have offered two responses to this analysis. First, commenters have pointed out that post-cut-through digits that are dialed for "transactional" purposes, such as digits that are dialed to conduct automated banking transactions, do not constitute "call-identifying information." We agree. Cf. USTA v. FCC,

227 F.3d at 462 (post-cut-through dialed digits entered for purposes such as automated banking "can * * * represent call content"). But the fact that post-cut-through transactional dialing is not "call-identifying information" is irrelevant to the question of whether post-cut-through telephone numbers – digits that identify the destination of the calling party's communication – are "call-identifying information." See Government Reply Comments at 38-40.

In this regard, we wish to emphasize that law enforcement is not seeking dialed digit extraction for the purpose of obtaining access to transactional dialing. As discussed below, we are not aware of any currently available technology that permits an originating carrier to limit dialed digit extraction to digits that are dialed for call routing purposes. But if and when such technology becomes available to carriers, we would have no objection whatsoever to its use – nor would we have any objection if the Commission were to modify the Third Report and Order to require carriers to use such technology. See p. 51 infra.

Second, some commenters have argued that because originating carriers do not themselves use post-cut-through digits for the purpose of routing outgoing calls, post-cut-through dialing does not constitute call-identifying information "for," or "from the perspective of," originating carriers, even when the dialed digits identify the number of the party that the subject is trying to reach. The central problem with this argument is that it ignores the actual language of CALEA. Neither the statutory definition of "call-identifying information" nor the terms of Section 103(a)(2) limit a carrier's obligation to call-identifying

information that is used by the carrier itself, as opposed to another carrier, for purposes of call processing.

As noted above, CALEA defines "call-identifying information" to mean "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." 47 U.S.C. § 1001(2). This definition manifestly is not a subjective or relative one. Nowhere does it ask whether dialing or signaling information is used by the particular carrier in question to route the communication. Instead, as long as dialing or signaling information "identifies the origin, direction, destination, or termination" of a "communication generated or received by a subscriber," it is "call-identifying information" -- period. Thus, post-cut-through digits that are dialed by a subscriber to identify the number of the party whom the subscriber is trying to reach constitute "call-identifying information" because they are "dialing or signaling information that identifies the destination" of a "communication generated * * * by a subscriber." There is no room in the statutory definition to exclude such information based on the use to which it is put by a particular carrier.[1]

---

[1] If the commenters' theory were correct, it would encompass not only post-cut-through

dialing, but also many kinds of pre-cut-through dialing. For example, when a subscriber dials a conventional inter-LATA long-distance call ("1-918-123-4567"), the originating carrier uses only the first few digits ("1-918") for purposes of routing the call to the subscriber's IXC. The commenters' theory implies that the originating carrier therefore could satisfy its obligations under CALEA by providing law enforcement with only a portion of the called party's number -- an obviously absurd result.

The language of Section 103(a)(2) is equally inhospitable to this line of argument. By its terms, Section 103(a)(2) obligates a carrier to provide the government with access to all "call-identifying information that is reasonably available to the carrier." If Section 103(a)(2) instead provided that a carrier is obligated to provide "call-identifying information that is reasonably available to the carrier and is used by the carrier to route the call," then the commenters' argument would have force. But the underscored words are not found in 103(a)(2); the commenters are simply asking the Commission to proceed as if they were. The actual language of Section 103(a)(2) makes clear that a carrier's obligation applies to all reasonably available call-identifying information, regardless of whether the carrier itself uses the information for call routing purposes.

C. The Other Punch List Capabilities

We now turn from dialed digit extraction to the other three punch list capabilities. In some respects – for example, in connection with party join/hold/drop information – the following discussion diverges from the analysis in the Third Report and Order. We respectfully encourage the Commission to consider our analysis in the Commission's review of the remaining punch list capabilities.

1. Subject-Initiated Dialing and Signaling

This capability provides law enforcement with access to dialing and signaling information that is generated when a subject uses services such as call forwarding, call waiting, call hold, and three-way calling. See Third Report and Order ¶ 76. To the extent that these services have been available in the POTS environment, law enforcement has

always had access to the subject-initiated dialing and signaling activity associated with them. Whenever a subject sends signals over the local loop to the carrier's switching equipment by pressing a key to direct, redirect, or otherwise manage incoming and outgoing calls, law enforcement is able to monitor and detect the signals through conventional pen register surveillance. See pp. 12-13 supra. If carriers are excused from continuing to provide this capability under CALEA, law enforcement will lose access to significant dialing and signaling activity to which it historically has had access. The Commission therefore should construe "call-identifying information" to encompass this kind of information unless there are compelling reasons to do otherwise.

As explained in our earlier filings, far from excluding such information, the definition of "call-identifying information" readily encompasses it. Government Whenever a subject presses a flash hook or feature key to manage incoming or outgoing communications, he is directing the communications. As explained above, "direction" is properly construed to encompass the subject's activities in directing communications. See pp. 15-16 supra. It follows that subject-initiated dialing and signaling information identifies the "direction" of "each communication" to and from the subject. See, e.g., Government Reply Comments at 45-47.

In addition, information about subject-initiated dialing and signaling activity can identify the "destination" of particular communications. For example, when a subject calls one party, then presses the flash hook to place the call on hold and accepts an incoming call from another party, the flash hook changes the destination of the ensuing communication.

In these circumstances, information about the subject's dialing and signaling activity identifies not only the subject's direction of the communication, but the destination of the communication as well.

2. In-Band and Out-of-Band Network Signaling

This capability provides law enforcement with access to signaling that is sent from the carrier's network to the subject's terminal in order to report the progress of incoming and outgoing call attempts. See Third Report and Order ¶ 83. With respect to outgoing call attempts, it includes such network-generated signaling as ringing signals and busy tones. With respect to incoming call attempts, it includes such network signaling as call-waiting tones, "stutter" tones, and signals that activate a message-waiting light.

This kind of network-generated signaling activity has traditionally been available to law enforcement through electronic surveillance on the "local loop" between the carrier and the subject. All network signals transmitted from the carrier to the subject across the local loop can be detected and decoded. For example, the equipment used to conduct pen register surveillance routinely records and reports ringing and busy signals on outgoing call attempts. Here again, the presumption in favor of maintaining law enforcement's traditional surveillance capabilities weighs heavily in favor of construing "call-identifying information" to include this kind of network-generated signaling.

Network signaling that reports the progress of outgoing call attempts constitutes "call-identifying information" because it identifies how the call attempt is being terminated by the called party's equipment, facilities, and services. A call attempt that results in a busy signal indicates that the call attempt is being terminated in a different manner from a call attempt that results in ringing. Busy signals and ringing permit law enforcement to "identify" these two different kinds of termination. Similarly, network signaling that reports the disposition

of incoming call attempts identifies how the incoming call attempt is terminated by the subject's own equipment, facilities, and services. In addition, network signaling regarding incoming call attempts may identify the direction of the call attempt by the subject's facilities; for example, a stutter tone may identify the fact that an incoming call has been redirected to the subject's voice mail box.[2]

3. Party Join/Hold/Drop Information

This capability requires carriers to notify law enforcement when a party to a multi-leg call is joined, dropped, or placed on hold. See Third Report and Order ¶ 68. This information falls squarely within the scope of "call-identifying information."

As explained above, the definition of "call-identifying information" includes information identifying (among other things) the direction and destination of "each communication generated or received by a subscriber." Whenever a subject adds a party to an existing call or a party is placed on hold or dropped from the call, the communication that ensues is different from the one that preceded it. For example, when a subject toggles back and forth

---

[2] It is undisputed that CALEA's definition of "call-identifying information" encompasses not only completed calls, but also unsuccessful call attempts. See, e.g., J-STD-025 § 5.4.8 (Release message "shall be triggered when a circuit-mode call attempt is abandoned by the calling party"); id. § 5.4.10 (TerminationAttempt message reports "an incoming circuit-mode call attempt to the intercept subject" and "shall be sent regardless of the disposition of the call (e.g., busy, answered, redirected)").

between two other parties in a three-way conference call, speaking first to one party and then to the other, the subject is engaged in two distinct communications. Information about the active leg(s) of the multi-party call identifies the subject's "direction" of each communication, and also identifies each the destination of each communication. See Government Reply Comments at 52-53; Second Government Reply Comments at 40-41.

We acknowledge, as we have from the outset of this proceeding, that this capability differs from the other punch list capabilities now at issue because some (although not all) of the information in question was unavailable to law enforcement in the POTS environment. See DOJ/FBI Joint Petition for Expedited Rulemaking ¶ 77, CC Docket No. 97-213 (filed March 27, 1998). Specifically, law enforcement was able to detect when new parties were joined to existing calls, but law enforcement could not directly detect when parties were placed on hold or were dropped from the call because that information resided in the switch. Ibid. Instead, law enforcement was left to infer which parties had been removed from the call (temporarily or permanently) by other means. As indicated above, the fact that law enforcement has not traditionally had access to particular information weighs against treating it as "call-identifying information." But the presumption that arises from law enforcement's historical lack of access is overcome in this context by the clear language of "call-identifying information" itself.

D. The J-Standard's Definition of "Call-Identifying Information"

As noted by the Court of Appeals, the J-Standard contains its own definition of "call-identifying information." The J-Standard's definition provides:

> call-identifying information [is] defined in CALEA Section 102(2) to be "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 [TSP]." As interpreted by this Interim Standard: destination 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).

J-STD-025, § 3 (emphasis in original).

As we have pointed out in previous filings, the J-Standard's definition of "call-identifying information" is flawed in several important ways. See, e.g., Government Reply Comments at 30-35. First, and most important, the J-Standard expressly construes "call-identifying information" to mean telephone numbers and nothing more. As we have explained, limiting "call-identifying information" to telephone numbers is not faithful to the language of the statute or the purposes of CALEA. See pp. 13-14 supra; USTA v. FCC, 227 F.3d at 458-459. Second, the J-Standard's interpretation of "direction" and "termination" makes those terms largely redundant with "origin" and "destination." See Government Reply Comments at 31-32. Third, the J-Standard's definition results in the exclusion of substantial amounts of information to which law enforcement has traditionally had access, such as most subject-initiated dialing and signaling activity and network-generated signals. For all of these reasons, the Commission should reject the J-Standard's definition of "call-identifying information" to the extent that it excludes the punch list capabilities at issue in this proceeding.

II. The Punch List Capabilities Satisfy the Cost Criteria of Section 107(b)

A. Introduction

Section 107(b) of CALEA sets forth the criteria to be followed by the Commission when it is called on to "establish * * * technical requirements or standards that meet the assistance capability requirements" of Section 103. Two of the statutory criteria in Section 107(b) involve cost considerations. First, subsection (b)(1) provides that the Commission's standards should meet Section 103's assistance capability requirements "by cost-effective methods." 47 U.S.C. § 1006(b)(1). Second, subsection (b)(3) provides that the Commission's standards should "minimize the cost of * * * compliance [with Section 103] on residential ratepayers." Id. § 1006(b)(3).

As noted above, the D.C. Circuit's decision requires the Commission to give further attention to the application of these cost criteria to the four punch list capabilities. As we now show, reinstating the punch list capabilities is fully consistent with the statutory cost criteria. The punch list capabilities represent "cost-effective methods" of meeting the assistance capability requirements of Section 103, and they do so in a way that will result in little if any cost to residential customers.

At earlier stages of this proceeding, the government faced severe limitations on its ability to present the Commission with information about CALEA implementation costs. Now, however, we are in a position to provide significant cost information that was previously unavailable. The information confirms that the Commission's original decision to add the four contested punch list capabilities to the J-Standard is fully consistent with the

cost criteria of Section 107(b). In particular, the record establishes three critical points, each of which we address in detail below.

First, from the standpoint of wireline and wireless carriers and their residential customers, the aggregate costs of implementing both the J-Standard and the punch list capabilities will be remarkably small. That is so because:

- the cost of implementing the J-Standard and the punch list capabilities is modest – an order of magnitude lower than the estimates offered by industry commenters earlier in this proceeding;
- the lion's share of those costs is being borne by the government, not by carriers or their customers; and
- to the maximum extent possible, carriers will be permitted to deploy CALEA solutions as part of their normal software upgrade cycle, eliminating costs that would otherwise arise if carriers were required to conduct additional upgrades in order to make their systems CALEA-compliant.

Second, the incremental costs associated with implementing the four contested punch list capabilities are much smaller than the aggregate costs of the J-Standard and the punch list. To the extent that wireline and wireless carriers will incur costs in making their systems CALEA-compliant, many of those costs will be the same regardless of whether the four contested punch list capabilities are added to the J-Standard or omitted from it. As a result, reinstating the four punch list capabilities will not result in significant costs to the carriers or their customers.

Third, even if the costs associated with implementing the four punch list capabilities were significantly higher than they actually are, the other commenters have thus far failed to identify any alternative measures that cure the deficiencies in the J-Standard by less expensive means, and that failure disposes of any cost-based objections under Section 107(b). As we have shown in previous filings, and as we explain further below, the cost criteria of Section 107(b) do not call on the Commission to decide whether the costs of particular assistance capabilities are worth incurring. That decision has already been made by Congress itself: the assistance capability requirements of Section 103 are mandatory ones, and nothing in Section 107(b) authorizes the Commission to excuse carriers from meeting those requirements. The cost criteria of Section 107(b) are directed instead at a more modest goal – ensuring that the Commission does not subject carriers and residential ratepayers to unnecessary expense by choosing a costly means of meeting Section 103's requirements when an equally effective but less expensive alternative is available. Here, the commenters have identified no alternatives at all for three of the four punch list capabilities, and their proposed alternatives for the fourth capability (dialed digit extraction) fail to qualify under Section 107(b) because they are inadequate to "meet the assistance capability requirements" of Section 103.

B. The Statutory Framework for CALEA Cost Recovery

When Congress enacted CALEA, it recognized that carriers might have to incur substantial costs in order to modify their systems to provide law enforcement with access to communications and call-identifying information. To minimize this potential financial

burden on carriers and their customers, Congress included several statutory provisions that permit carriers to recover CALEA-related costs from the federal government. See generally USTA v. FBI, No. 98-2010, slip op. 2-9 (D.D.C. Aug. 28, 2000), appeal pending, No. 00-5386 (D.C. Cir.) (summarizing CALEA cost recovery provisions). We begin by briefly reviewing the statutory framework for CALEA cost recovery.

1. Assistance Capability Costs

With regard to equipment, facilities, and services that were installed or deployed before January 1, 1995, CALEA provides for the federal government, rather than telecommunications carriers, to bear the cost of meeting CALEA's assistance capability requirements. Section 109(a) of CALEA authorizes the Attorney General, subject to the availability of appropriations, to pay telecommunications carriers for "all reasonable costs directly associated with the modifications performed by carriers in connection with equipment, facilities, and services installed or deployed on or before January 1, 1995, to establish the [assistance] capabilities" required by CALEA. 47 U.S.C. § 1008(a). If the Attorney General chooses not to pay for modification of particular pre-1/1/95 equipment, the equipment is deemed to in compliance with the assistance capability requirements until it is replaced or significantly upgraded or otherwise undergoes major modification. Id. § 1008(d).

With respect to equipment, facilities, and services that have been installed or deployed *after* January 1, 1995, the financial responsibility for meeting CALEA's assistance capability requirements generally rests on carriers themselves. However, a carrier that finds it prohibitively expensive to bring particular post-1/1/95 equipment, facilities, or services

into compliance may petition the Commission for a determination that compliance is not "reasonably achievable." 47 U.S.C. § 1008(b); see generally In the Matter of Communications Assistance for Law Enforcement Act, Second Report and Order ¶¶ 30-46, CC Docket No. 97-213 (released Aug. 31, 1999). In determining whether compliance is reasonably achievable, the Commission must consider whether compliance "would impose significant difficulty or expense on the carrier or on the users of the carrier's systems." 47 U.S.C. § 1008(b)(1). In addition, the Commission must consider "[t]he effect on rates for basic residential telephone service," "[t]he effect on the nature and cost of the equipment, facility, or service at issue," and "[t]he financial resources of the telecommunications carrier." Id. § 1008(b)(1)(B), (E), (H); see Second Report and Order ¶¶ 42-43. If the Commission determines that compliance is not "reasonably achievable" in light of these and other statutory criteria, the equipment, facilities, or services in question are deemed to be in compliance with CALEA's assistance capability requirements unless the Attorney General agrees to pay for "the additional reasonable costs of making compliance with such assistance capability requirements reasonably achievable." 1008(b)(2).

2. Capacity Costs

In order for a carrier to assist law enforcement in the performance of lawful electronic surveillance, not only must the carrier have the *capability* to provide access to communications and call-identifying information, but depending on the needs of law enforcement in a particular area, the carrier also may need the *capacity* to accommodate multiple interceptions simultaneously. In addition to providing for the federal government

to bear a share of industry's assistance capability costs, CALEA also provides for the government to assume responsibility for the cost of modifying systems to meet law enforcement's capacity requirements.

Section 104(a) of CALEA provides for the Attorney General to issue capacity notices that tell carriers that actual and maximum number of simultaneous interceptions that law enforcement agencies expect to conduct in particular areas. 47 U.S.C. §§ 1003(a), 1003(c)(1). Carriers are required to ensure that their systems are capable to accommodating the number of simultaneous interceptions specified in the capacity notices. Id. §§ 1003(b), 1003(c)(2). Any carrier whose system does not meet the capacity requirements may submit a statement to the Attorney General identifying the system within 180 days of the publication of the capacity notice. Id. § 1003(d). The Attorney General may, subject to the availability of appropriations, agree to reimburse a telecommunications carrier for reasonable costs directly associated with modifications to attain the capacity requirements. Id. § 1003(e). If the Attorney General does not reimburse the carrier for such modifications, the carrier shall be considered to be in compliance with the capacity notices. Ibid.

3. Cost Recovery Regulations

Section 109(e) of CALEA authorizes the Attorney General to issue regulations providing for "timely and cost-efficient payment to telecommunications carriers under this subchapter." 47 U.S.C. § 1008(e)(1). Section 109(e) provides that the regulations shall permit recovery from the federal government of:

> (1) the direct costs of modifying pre-1/1/95 equipment to meet the assistance capability requirements of Section 103;
>
> (2) the direct costs of modifying post-1/1/95 equipment with respect to which compliance with Section 103 is otherwise not "reasonably achievable";
>
> (3) the direct costs of providing the capacities requested under Section 104.

47 U.S.C. § 1008(e)(2)(A)(i). Section 109 also provides that the regulations shall permit recovery of the direct costs of deploying and installing such capabilities and capacities and any associated training costs. Id. § 1008(e)(2)(A)(ii)-(iii).

The Department of Justice has issued cost recovery regulations that provide for reimbursement of the costs specified in Section 109(e). See 28 C.F.R. Part 100. If the appropriation currently recommended in Conference Report H.R.106-1005 is enacted, as anticipated, Congress will provide $500 million to the Department of Justice for reimbursement of allowable costs under Section 109(e) and the cost recovery regulations.

C. The Costs of Implementing the Punch List Capabilities

We now turn from the legal framework governing CALEA cost recovery to the factual record regarding CALEA implementation costs. At the outset, we wish to emphasize one

point: what matters for present purposes is the cost of implementing the four punch list capabilities that are now at issue in this proceeding, not the total cost of CALEA compliance. As explained below, certain CALEA implementation costs will be incurred regardless of whether the four punch list capabilities are reinstated or not. These costs are inherent in the process of making equipment CALEA-compliant, and would be incurred even if the J-Standard were left in its original form. Because the punch list capabilities are not the source of these costs, such costs are irrelevant to the Commission's application of Section 107(b)'s cost criteria to the punch list capabilities themselves.

1. Acquisition Costs

a. In order for a carrier to bring its switching equipment into compliance with the assistance capability requirements of CALEA, the manufacturer must develop and provide software that implements the required assistance capabilities within the switch. The government has engaged in negotiations with switch manufacturers and carriers to develop CALEA-compliant solutions for the principal switch platforms used by the Nation's wireline and wireless carriers. Thus far, these negotiations have led to cooperative agreements between the government and four major switch manufacturers, along with carrier partners for each of the manufacturers. The four manufacturers who have entered into cooperative agreements thus far are AGCS, Lucent, Nortel, and Siemens. The government is currently engaged in negotiations with a fifth manufacturer as well.

Under the terms of the cooperative agreements, the manufacturer undertakes to provide a CALEA-compliant software solution for a designated switch platform, such as

Lucent's 5ESS switch. In each case, the manufacturer is obligated to provide software that includes the features of the J-Standard and all of the punch list capabilities added to the J-Standard by the Third Report and Order. With respect to each platform, the cooperative agreement specifies a total price, the portion of the price to be paid upon delivery of the J-Standard features, and the portion of the price to be paid upon delivery of the punch list capabilities.

The following table lists the switch platforms covered by the cooperative agreements, the contract price for each platform, and the allocation of the total price between the J-Standard features and the punch list capabilities:

Manufacturer	**Platform***	**Platform Price**	**J-Standard Price**	**Punch list price**
AGCS	GTD-5	$30,000,000	$25,000,000	$5,000,000
Lucent	*Autoplex 1000*	$60,000,000	$54,000,000	$6,000,000
	5ESS	$110,000,000	$95,000,000	$15,000,000
Nortel	DMS-10	$20,900,000	$18,000,000	$2,900,000
	DMS-100	$30,000,000	$25,000,000	$5,000,000
	DMS-MTX	$33,000,000	$26,000,000	$7,000,000
	DMS-MSC	$17,900,000	$13,400,000	$4,500,000
Siemens	DCO	$20,000,000	$15,000,000	$5,000,000

Manufacturer	Platform*	Platform Price	J-Standard Price	Punch list price
	EWSD	$20,000,000	$15,000,000	$5,000,000

* Wireline platforms in regular typeface, wireless platforms in italics

These switch platforms account for approximately 85 percent of the wireline and wireless switches currently in use in the United States. The total price for the CALEA software solutions for these platforms is $346.8 million. That figure is vastly lower – by an order of magnitude – than the estimates offered by commenters in earlier stages of this proceeding. See, e.g., Third Report and Order ¶ 20 (CTIA estimates total cost of more than $4 billion; PCIA estimates cost of more than $1.7 billion for J-Standard alone).

Equally striking is the small share of the cost attributable to the punch list capabilities. The cumulative amount paid under all of the agreements for the six punch list capabilities approved by the Third Report and Order is barely 16 percent of the total amount – roughly $55 million out of a total of almost $350 million. The Lucent 5ESS license is representative: the punch list capabilities cost only $15 million, less than 15 percent of the total price of $110 million.

Most important of all for present purposes, the cost of the CALEA solutions provided under the cooperative agreements is borne entirely by the federal government. Under the terms of each cooperative agreement, the manufacturer's carrier partner pays an agreed-upon price to purchase a "right-to-use" (RTU) license for the CALEA software solution. The government undertakes to reimburse the carrier partner in full for the cost of the RTU

license. In addition, the manufacturer agrees to grant the same RTU license without charge to all other carriers who are using the switch platform, and to do so not only for "grandfathered" switches installed or deployed before January 1, 1995, but also for switches installed or deployed after that date. As a result, every carrier in the United States who is using the switch platform is entitled to receive software that implements the J-Standard and the punch list capabilities – including the four punch list capabilities currently at issue in this proceeding – at no charge.

b. With respect to some switch platforms, the CALEA solution requires hardware modifications as well as new software. However, with minor exceptions, the required hardware modifications are not attributable to the four punch list capabilities. For example, some carriers may be required to install new processors in their switches to accommodate the features added by the J-Standard. Having done so, they will not have to make additional processor changes to accommodate the further features added by the punch list.

One of the punch list capabilities, dialed digit extraction, may require additional hardware for certain switch platforms. However, to the extent that hardware add-ons for dialed digit extraction are attributable to capacity requirements (i.e., the volume of simultaneous intercepts that the carrier must be capable of handling under the capacity notices), carriers may seek reimbursement under the capacity provisions of the Department's cost recovery regulations. Moreover, because CALEA "grandfathers" pre-1/1/95 switches, the cost of any hardware modifications required to implement dialed digit extraction on pre-1/1/95 switches will not be borne by carriers.

2. Deployment Costs

Whenever a carrier installs new software to expand or enhance a switch's features, the carrier incurs deployment costs, such as the cost of testing the new software package and the cost of training personnel to use and administer the new features. To minimize these costs, carriers ordinarily deploy software upgrades on a regular business cycle. If a new feature is deployed as part of a regularly scheduled upgrade, the incremental deployment costs attributable to the feature are ordinarily small, and in some cases virtually non-existent. In contrast, if the new feature is deployed through a separate upgrade that is not part of the carrier's regular deployment cycle, the deployment costs can be more significant.

To assist carriers in reducing the deployment costs associated with CALEA implementation, the government has sponsored a "flexible deployment" program. The goal of the flexible deployment program is to permit carriers to deploy CALEA-compliant solutions in accordance with their normal generic upgrade cycle, where such deployment will not impede implementation of CALEA solutions in areas of high priority to law enforcement.

Carriers wishing to participate in the flexible deployment program provide the government with projected CALEA deployment schedules for all switches in their network, as well as information pertaining to any recent lawfully-authorized electronic surveillance activity. Using this information, the government and the carrier attempt to develop a mutually agreeable deployment schedule. This approach provides an opportunity for carriers and the government to agree on deferring the installation of CALEA-compliant solutions in those

instances where public safety and national security would not be jeopardized. If the government and the carrier are able to agree upon a deployment schedule, the government will support a petition by the carrier under Section 107(c) of CALEA to extend the existing assistance capability compliance deadline of June 30, 2000, for the core J-Standard.[3]

Approximately 1,250 carriers have submitted flexible deployment applications to the government relating to the compliance deadline. Thus far, the government has approved flexible deployment schedules for approximately 920 of these carriers and has agreed to support their extension petitions under Section 107(c). No carrier has been turned down; the applications of the remaining carriers have not been acted on yet and remain under review.

The flexible deployment program greatly reduces the deployment costs that would otherwise be incurred if CALEA features had to be deployed outside of a carrier's regular generic upgrade cycle. Under a typical flexible deployment schedule, the J-Standard features will be deployed as part of one regularly scheduled generic upgrade, and the punch list capabilities will be deployed as part of a subsequent regularly scheduled upgrade. Because the CALEA capabilities are part of a generic software package that must be deployed in any

---

[3] The flexible deployment program is summarized in Public Notice 00-154, CALEA Section 103 Compliance and Section 107(c) Petitions, CC Docket No. 97-213 (released April 25, 2000). The CALEA Implementation Section of the FBI has issued a "Flexible Deployment Assistance Guide" that describes the flexible deployment program in detail. The guide is available at <http://www.askcalea.net/pdf/flexguide.pdf>.

case, the additional deployment costs attributable to the CALEA features themselves are small, and the incremental deployment costs associated with the four contested punch list capabilities are smaller still.

3. Capacity Costs

In some cases, carriers may be required to modify their equipment to meet the capacity requirements of Section 104 of CALEA. As explained above, carriers who submit appropriate documentation are eligible to be reimbursed for the reasonable costs directly associated with modifications required to meet the capacity requirements, and if reimbursement is not forthcoming, the carrier is deemed to be in compliance with the applicable capacity notices. 47 U.S.C. §§ 1003(d)-(e). As a result, neither carriers nor their customers will be required to bear the costs of CALEA's capacity requirements.

D. Applying the Cost Criteria of Section 107(b)

In the Third Report and Order, the Commission undertook to apply the cost criteria of Section 107(b) by estimating the costs of the punch list capabilities and comparing them to the costs associated with the J-Standard. See, e.g., Third Report and Order ¶ 30. The Court of Appeals dismissed the Commission's approach as inadequate, stating that "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 exhorbitant,' nor finally what impact it thought the Order would have on residential ratepayers." 227 F.3d at 461-462.

To address the shortcomings identified by the Court of Appeals, the Commission must begin by considering the purpose of the cost criteria in Section 107(b). As we now

show, the cost criteria are designed to serve a limited purpose, and once that purpose is identified and borne in mind, it becomes readily apparent why the vacated punch list capabilities satisfy the cost criteria.

The general object of Section 107(b) is to ensure that carriers compliance with CALEA's assistance capability requirements, by correcting deficiencies in industry standards that would otherwise provide a "safe harbor" under Section 107(a)(2). The purpose of proceedings under Section 107(b) is not to decide whether carriers must comply with the assistance capability requirements of Section 103, but instead to decide how they are to comply. Section 107(b) thus stands in marked contrast to the "reasonable achievability" provisions of Section 109(b), which are designed to excuse individual carriers from compliance where costs or other factors render compliance not "reasonably achievable" unless the federal government assumes the costs of compliance.

In keeping with the overall purpose of Section 107(b), the cost criteria of Section 107(b) direct the Commission to take account of cost in determining how the assistance capability requirements of Section 103 are to be met, not whether they are to be met. Specifically, the Commission is directed to look for "cost-effective means" of "meet[ing] the assistance capability requirements" and to "minimize the cost of * * * compliance" with those requirements. 47 U.S.C. §§ 1006(b)(1), 1006(b)(3) (emphasis added). By their terms, these provisions presuppose that any technical standards adopted by the Commission will "meet" the requirements of Section 103 and ensure "compliance" with those requirements.

Accordingly, the cost provisions of Section 107(b) do not authorize the Commission to adopt technical standards that fail to "meet the assistance capability requirements of section 103" because of freestanding concerns about cost. Section 109(b), with its precisely articulated factors for determining whether compliance is "reasonably achievable," is the avenue provided by Congress for the Commission to excuse carriers from compliance. Congress has made a global determination that the benefits of requiring carriers to meet Section 103's assistance capability requirements exceed the costs. Section 107(b) is not intended to invite an administrative reconsideration of that quintessentially legislative cost-benefit determination.[4]

Instead of requiring the Commission to weigh the financial costs of a particular capability to carriers and residential ratepayers against the social benefits of the capability

[4] It should be noted in this regard that Section 109(b), in contrast to Section 107(b), directs the Commission to take account of "[t]he effect on public safety and national security." See 47 U.S.C. 1008(b)(1)(A). If Section 107(b) were meant, like Section 109(b), to be a vehicle for excusing carriers from compliance with their assistance capability obligations, Congress would have included the same directive in Section 107(b), in order to ensure that the private costs of compliance are balanced against the public costs of non-compliance. Because Section 107(b) is not designed to excuse carriers from compliance with CALEA's assistance capability requirements, there was no need for Congress to direct the Commission to consider the costs to "public safety and national security" from non-compliance.

to law enforcement and the public at large, Section 107(b)'s cost criteria call for a far more modest and manageable form of weighing – a comparison of the relative costs of alternative methods of meeting the assistance capability requirements of Section 103. If there is more than one means of complying with the assistance capability requirements, then the Commission may take account of relative costs, along with the other factors in Section 107(b), in choosing among the alternatives. But if no alternatives exist, or if purported alternatives do not in fact "meet the assistance capability requirements" of Section 103, then the cost inquiry is at an end.

Once these principles are recognized, the application of Section 107(b)'s cost criteria to the four contested punch list capabilities becomes straightforward. As explained in our earlier filings, commenters have not identified any alternatives, much less any cheaper alternatives, for three of the four punch list capabilities – subject-initiated dialing and signaling, in-band and out-of-band network signaling, and party join/hold/drop information. And while commenters have suggested alternatives to dialed digit extraction, the proposed alternatives are themselves inconsistent with Section 107(b), because they do not "meet the assistance capability requirements" of Section 103. See Government Reply Comments at 41-42 & n.24; Second Government Reply Comments at 62-64. We address the proposed alternatives to dialed digit extraction in greater detail in Part III of our comments. See pp. 52-55 infra.

In sum, the Commission acted entirely in keeping with the cost criteria of Section 107(b) when it added the four punch list capabilities to the J-Standard. The Commission

properly determined in the original proceeding that the J-Standard is deficient and that punch list capabilities will eliminate the deficiencies. Having made those determinations, the only question posed by Section 107(b)'s cost criteria is whether there are equally effective but less expensive alternatives. Because no such alternatives have been shown to exist, adopting the punch list capabilities is consistent with the cost criteria of Section 107(b). Moreover, given the factual record set forth above regarding the minimal costs associated with implementing the punch list capabilities, the same conclusion would follow even if, contrary to our submission, Section 107(b) did call on the Commission to gauge the absolute magnitude of the costs associated with the punch list capabilities and to make a more general cost-benefit determination.

III. The Punch List Capabilities Satisfy the Privacy Criterion of Section 107(b)

A. Dialed Digit Extraction

In addition to finding that the Commission had not adequately explained its application of Section 107(b)'s cost criteria, the Court of Appeals also found that the Commission had not adequately explained its treatment of Section 107(b)(2), which calls on the Commission to adopt standards that "protect the privacy and security of communications not authorized to be intercepted." 47 U.S.C. § 1006(b)(2). The Court of Appeals found no fault with the Commission's application of this provision to three of the four contested punch list capabilities. However, the court found that the Commission had not adequately explained how dialed digit extraction satisfies Section 107(b)(2). 227 F.3d at 462-463. As the Commission itself noted in the Third Report and Order, dialed digit extraction results in

the delivery not only of post-cut-through digits that are dialed for call routing purposes, but also post-cut-through digits that are dialed for other purposes such as telephone banking or automated credit card transactions. The Court of Appeals concluded that the delivery of non-routing digits raises potential privacy issues that the Commission did not adequately address. Ibid.

As we now show, dialed digit extraction is consistent with Section 107(b)(2). Dialed digit extraction does not result in the unauthorized delivery of "communications not authorized to be intercepted," because the delivery of post-cut-through dialed digits to law enforcement is specifically contemplated by the pen register statute and CALEA itself. Moreover, the alternatives to dialed digit extraction that have been proposed by other commenters are themselves inconsistent with Section 107(b), because they do not ensure that carriers will (in the words of Section 107(b)(1)) "meet the assistance capability requirements" of CALEA.

1. Dialed Digit Extraction and Federal Electronic Surveillance Law

a. The privacy-based objections to dialed digit extraction assume that the pen register statute (18 U.S.C. §§ 3121-3127) does not authorize carriers to deliver post-cut-through dialed digits to law enforcement, because the stream of post-cut-through digits may contain digits that have been dialed for non-call routing purposes. That assumption is incorrect.

As explained above, law enforcement agencies performing electronic surveillance in the POTS environment traditionally have received all dialing and signaling activity

transmitted across the local loop, including post-cut-through as well as pre-cut-through dialed digits. If the commenters were correct that the delivery of post-cut-through dialed digits exceeds the scope of the pen register statute, then virtually every instance of pen register surveillance in the POTS environment would be unlawful, since law enforcement routinely receives post-cut-through digits in such cases. Fortunately, the commenters' position is flatly inconsistent with the terms of the pen register statute itself. In particular, the commenters' position conflicts with 18 U.S.C. 3121(c) – a provision added to the pen register statute by CALEA itself.

Section 3121(c) provides:

> A government agency authorized to install and use a pen register under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing. [Emphasis added.]

The legislative history of CALEA makes clear that Congress added Section 3121(c) to the pen register statute specifically to address the present scenario -- one in which law enforcement receives not only "dialing or signaling information necessary to direct or process a call," but also "communication[s] conducted through the use of dialed digits." House Report at 32, reprinted in 1994 USCCAN at 3512. Congress's response to this phenomenon was not to prohibit carriers from delivering post-cut-through dialed digits in pen register cases. Instead, Congress chose to require law enforcement agencies to "use, when

reasonably available, technology that restricts the information captured" to call processing information. Ibid. Section 3121(c) presupposes that a carrier is not acting unlawfully under the pen register statute when it delivers post-cut-through digits that include (or may include) transactional information as well as phone numbers. If carriers were not authorized to deliver post-cut-through digits in the first place, as the commenters have suggested, there would be no reason for Congress to enact Section 3121(c), which addresses how a law enforcement agency should handle post-cut-through digits when it receives them. Because the delivery of post-cut-through digits is authorized under the pen register statute, law enforcement is not required to obtain a Title III interception order in order to acquire such dialing information. See 18 U.S.C. § 2511(2)(h) (excluding pen register surveillance from requirements of Title III).

b. The government's views regarding the applicability of the pen register statute to post-cut-through dialed digits have been disputed by other parties to this proceeding, and the Court of Appeals noted that the issue is one that has not yet been addressed by the courts. See USTA v. FCC, 227 F.3d at 462. However, the Commission does not have to reach a conclusive resolution of the issue in order to reinstate dialed digit extraction. Instead, there are measures that the Commission can take that will serve to "protect the privacy and security of communications not authorized to be intercepted" in the event that a courts ultimately differs with the government regarding the scope of the pen register statute.

First, the Commission can hold squarely that, while carriers must have the capability to perform dialed digit extraction, no carrier is required to deliver post-cut-through digits in

the absence of appropriate legal authorization. By making clear that its decision is directed solely at the issue of capability, not that of legal authorization, the Commission can ensure that carriers do not mistakenly regard themselves as "bound" by the Commission's order to deliver post-cut-through digits. If a court determines that the pen register statute does not provide sufficient legal authority for a carrier to perform dialed digit extraction, the Commission's decision would not preclude such a determination.

Second, the Commission can require a carrier to have the capability to "turn off" dialed digit extraction in pen register cases if and when a court determines that the pen register statute does not provide sufficient legal authority for the carrier to use this capability. Many of the CALEA software solutions that have been developed pursuant to the cooperative agreements provide carriers with the ability to toggle individual punch list capabilities on and off. With respect to these solutions, adding dialed digit extraction to the J-Standard will not have the effect of forcing a carrier to use the feature if the carrier has reservations about the legal basis for delivering post-cut-through dialed digits. Any such carrier that believes that dialed digit extraction is beyond the scope of the authority conferred by the pen register statute may seek relief from a pen register order, and if the court concludes (contrary to the government's view) that the pen register statute does not provide authority for the delivery of post-cut-through digits, the carrier would have the ability to turn off dialed digit extraction before executing the pen register order.[5] If the Commission wishes

[5] Although the scope of judicial review of pen register applications is limited, courts retain the power to "ensur[e] compliance with the statutory requirements established by Congress"

to do so, it can modify the Third Report and Order to make this toggling capability a condition for dialed digit extraction, thereby ensuring that carriers can execute pen register orders without jeopardizing "the privacy and security of communications not authorized to be intercepted" if a particular court differs with the government regarding the legality of acquiring post-cut-through digits under the pen register statute.

Third, the Commission can modify the Third Report and Order to take account of the possibility that originating carriers may one day be able to distinguish between post-cut-through digits entered for call routing purposes and post-cut-through transactional digits. To our knowledge, no such "filtering" technology exists today, but it may become available in the future. If such technology were already in existence, Section 107(b)(2) presumably would permit the Commission to require the deployment of such a capability in pen register cases, thereby withholding transactional digits while continuing to provide law enforcement with access to call routing digits. Given the possibility that such technology may become available in the future, the Commission may wish to modify the Third Report and Order now by requiring carriers to employ such technology if and when it becomes available.

---

under the pen register statute. United States v. Hallmark, 911 F.2d 399, 402 (10th Cir. 1990). If a law enforcement agency invokes the pen register statute to seek information that is outside the scope of the statute, it would not be acting in "compliance with the statutory requirements established by Congress," and the court would be free to decline to issue the order, or to grant a motion to quash an already-issued order, on that ground.

Nevertheless, in the absence of such technology, dialed digit extraction is a permissible solution to the J-Standard's failure to deliver post-cut-through digits.

2. Alternatives to Dialed Digit Extraction

As noted above, commenters have previously proposed alternatives to dialed digit extraction as means of providing law enforcement with access to post-cut-through digits that are dialed for call routing purposes. Two proposals have received particular emphasis. First, some commenters have suggested that law enforcement agencies can obtain post-cut-through digits by obtaining an interception order under Title III, 18 U.S.C. § 2518. Second, commenters have suggested that law enforcement can collect post-cut-through digits by serving pen register orders on "downstream" carriers that utilize the digits for call processing purposes. The commenters have argued that both of these alternatives provide law enforcement with access to post-cut-through digits without delivering transactional digits in pen register cases.

We agree with the commenters that these alternatives satisfy Section 107(b)(2) – as does dialed digit extraction itself. But the alternatives do not satisfy the other criteria of Section 107(b). In particular, they fail to meet the threshold requirement of Section 107(b) – namely, that the Commission's technical standards "meet the assistance capability requirements" of Section 103. If the Commission were to adopt either of these purported alternatives, law enforcement would not receive access to all reasonably available call-identifying information, as required by Section 103(a)(2) (47 U.S.C. § 1002(a)(2)), nor would it be assured of receiving such information "before, during, or immediately after the transmission" of the communication, as required by Section 103(a)(2)(A) (id.

§ 1002(a)(2)(A)). We have addressed this problem in our prior comments; we summarize those comments here.

With respect to the first alternative, the legal requirements for obtaining an interception order under Title III are, quite appropriately, far more demanding than the requirements for obtaining a pen register order. Under Title III, law enforcement must have probable cause that a person is committing or has committed specified crimes; probable cause that particular communications concerning the crime will be obtained through the interception; probable cause that the facilities to be surveilled are being used in connection with the commission of the crime or are commonly used by the suspect; and proof that normal investigative procedures have been exhausted, are unlikely to succeed, or are too dangerous. 18 U.S.C. § 2518(3)(a)-(d). In contrast, law enforcement is entitled to a pen register order if it certifies that the information likely to be obtained by installing and using a pen register "is relevant to an ongoing criminal investigation." Id. § 3123(a).

Given the dramatic difference in these legal standards, there are thousands of cases in which law enforcement is able to obtain a pen register order but would not be able to meet the requirements of an interception order under Title III. In all of these cases, the "solution" of requiring a Title III order would deny law enforcement access to post-cut-through digits that are dialed for call routing purposes, even though law enforcement has a court order under the pen register statute that entitles it to obtain such information. That result is squarely inconsistent with Section 103(a)(2) of CALEA, which obligates carriers to provide law enforcement with access to all reasonably available call-identifying information for

which law enforcement has "a court order or other lawful authorization." 47 U.S.C. § 1002(a)(2).

Moreover, requiring a Title III order for the delivery of post-cut-through dialed digits would turn CALEA into a Catch-22 for law enforcement. Given the demanding standards imposed by Title III, interception orders are rarely issued without the presentation of evidence derived from pen registers and trap-and-trace devices. If law enforcement cannot obtain access to post-cut-through digits without a Title III order, it may be prevented from gathering the very evidence that is needed to obtain a Title III order in the first place. Thus, not only would this alternative prevent law enforcement from engaging in lawful surveillance under the pen register statute, but it would effectively impair law enforcement's ability to proceed under Title III itself.

The second alternative, that of requiring law enforcement to serve pen register orders on downstream carriers, would inevitably result in the loss of call-identifying information that carriers are obligated to provide under Section 103(a)(2). As we have explained in our earlier filings, many potential downstream carriers, such as carriers who provide long-distance calling-card services, do not maintain records of long-distance numbers once the call is complete, since their billing rates are not tied to the destination of the call. In those cases, remitting law enforcement to the downstream carrier is tantamount to denying law enforcement access to the dialed digits altogether. Moreover, even when a downstream carrier does maintain dialing records for billing purposes, law enforcement will not be able to obtain the information until long after the call is complete – for example, by serving a

subpoena or an order under 18 U.S.C. § 2703(c)-(d). Section 103(a)(2)(A) entitles law enforcement to receive call-identifying information contemporaneously with the communication to which it relates; that requirement cannot possibly be satisfied if law enforcement is compelled to look to downstream carriers for the information.

Our point in identifying the deficiencies in these alternatives is not to suggest that they entitle the Commission to disregard any privacy concerns raised by dialed digit extraction. See USTA v. FCC, 227 F.3d at 462 (Commission's reliance on problems associated with alternatives to dialed digit extraction is an "unsatisfactory response to CALEA's privacy provisions"). If dialed digit extraction were inconsistent with Section 107(b)(2), then the Commission would not be at liberty to add it to the J-Standard, regardless of the shortcomings of the alternatives. But as shown above, dialed digit extraction is consistent with Section 107(b)(2). That being the case, there is no warrant for the Commission to adopt alternative measures unless the alternatives themselves satisfy to the criteria of Section 107(b), including the requirement that they "meet the assistance capability requirements" of Section 103. Here, the proposed alternatives simply do not do so.

B. The Other Punch List Capabilities

As noted above, the D.C. Circuit did not call into question the Commission's application of Section 107(b)(2) to the three other punch list capabilities. There is no reason why the Commission should depart from its original decision in this regard.

Each of the types of information covered by the remaining punch list capabilities is used by carriers in the course of call processing, and each therefore comes within the scope of the pen register statute as "dialing and signaling information utilized in call processing" (18 U.S.C. 3121(c)). Moreover, while these kinds of information are not telephone numbers, they share the attributes of phone numbers that are essential for purposes of the pen register statute. A telephone user lacks a reasonable expectation of privacy in dialing and signaling information that he transmits "to [the carrier's] equipment in the ordinary course of business" (Smith, 442 U.S. at 744) for call processing purposes, and a fortiori, he lacks an expectation of privacy in dialing and signaling information that is generated by the carrier's equipment itself. See USTA v. FCC, 227 F.3d at 459.

As a result, acquisition of such information is entirely consistent with the logic of the pen register statute. Moreover, even if law enforcement could not obtain this kind of information pursuant to a pen register order, it unquestionably could do so pursuant to other sources of authority like Title III and Rule 41 of the Federal Rules of Criminal Procedure. Accordingly, adding these capabilities to the J-Standard, subject to the statutory requirement that law enforcement have "lawful authorization" to obtain such information (47 U.S.C.

§§ 1002(a)(1)-(2)), poses no threat to the "privacy and security of communications not authorized to be intercepted."

IV. The Commission's Technical Standards Should be Modified in Several Respects

As the foregoing discussion illustrates, the Commission has an ample legal basis for reinstating the punch list capabilities that were vacated by the Court of Appeals. The punch list capabilities are consistent with CALEA's definition of "call-identifying information" and the cost and privacy criteria of Section 107(b). As long as the Commission provides a more thorough explanation of its grounds for adding the punch list capabilities to the J-Standard, the Commission's decision will satisfy the terms of the D.C. Circuit's remand.

In so doing, however, the Commission should consider the advisability of several modifications to the Third Report and Order. The primary purpose of these suggested modifications is not to alter the substance of the Commission's decision, but rather to clarify its intended scope and operation.

A. The Effect of the Commission's Standards

The first suggested clarification involves the legal effect of the Commission's standards. By virtue of CALEA's safe-harbor provision (47 U.S.C. § 1006(a)(2)), any carrier can bring itself into compliance with CALEA's assistance capability requirements by meeting technical standards adopted by industry or the Commission. A carrier that satisfies the assistance capability requirements of Section 103 of CALEA by means other than those specified in industry or Commission safe-harbor technical standards is under no obligation

to conform to the safe-harbor standards themselves – provided that the carrier is, in fact, complying with the underlying requirements of Section 103.

To avoid any potential confusion on this score, the Commission should modify the Third Report and Order to make clear that the Commission's technical standards provide carriers with one alternative for meeting their assistance capability obligations. At the same time, the Commission should make clear that a wireline, cellular, or broadband PCS carrier that fails to comply with the Commission's standards is ineligible for the shelter of CALEA's safe-harbor provision and remains subject to the underlying requirements of Section 103. We therefore suggest that the Commission add a provision such as the following one:

> A telecommunications carrier that provides the capabilities set forth in this rule, together with the capabilities set forth in J-STD-025 or any revision to J-STD-025, satisfies the safe-harbor requirements of 47 U.S.C. § 1006(a)(2). A carrier that complies in full with the underlying assistance capability requirements of 47 U.S.C. § 1002(a) is not under an independent obligation to comply with this rule. However, a carrier that does not comply with this rule does not satisfy the requirements of 47 U.S.C. § 1006(a)(2) and remains subject to the requirements of 47 U.S.C. § 1002(a).

B. The Distinction Between Assistance Capability and Legal Authority

The second clarification concerns the distinction between a carrier's technical capability to provide information to law enforcement and law enforcement's legal authority to obtain information from the carrier. CALEA's assistance capability requirements are directed solely at the question of what information a carrier must be capable of providing to

law enforcement when presented with a court order or other lawful authorization – not the separate question of what information law enforcement is entitled to obtain in any particular case. The Commission should make clear that its order addresses only the former question, not the latter one, and that the order should not be misconstrued to compel the delivery of information in the absence of proper legal authorization. We therefore recommend that the Commission add a provision such as the following one:

> The provisions of this rule concern the assistance capabilities that a telecommunications carrier must have when presented with a court order or other lawful authorization for the interception of communications and/or the acquisition of call-identifying information. Nothing in this rule shall be deemed to compel a telecommunications carrier to provide communications or call-identifying information to a law enforcement agency in the absence of a court order or other lawful authorization.

C. The J-Standard Definition of "Call-Identifying Information"

The final suggested clarification concerns the J-Standard's definition of "call-identifying information." For reasons set forth above, the J-Standard's definition is unduly restrictive. By adding the punch list capabilities to the J-Standard, the Commission implicitly superseded that definition, but the Commission did not do so explicitly. To make clear that the J-Standard's definition of "call-identifying information" is subordinate to the Commission's decision regarding the punch list capabilities, we recommend that the Commission add a provision such as the following one:

> To the extent that the definitions of "call-identifying information" and its constituent terms (such as "origin," "direction," "destination," and "termination") in J-STD-025 or any revision of

J-STD-025 are inconsistent with the provisions of this rule, this rule supersedes such definitions.

DATE: November 16, 2000

Respectfully submitted,

Louis J. Freeh, Director
Federal Bureau of Investigation

Honorable Janet Reno
Attorney General of the United States

William B. Schultz
Deputy Assistant Attorney General

Larry R. Parkinson
General Counsel
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

Douglas N. Letter
Appellate Litigation Counsel
Civil Division
U.S. Department of Justice
601 D Street, N.W., Room 9106
Washington, D.C. 20530
(202) 514-3602

Certificate of Service

I, Myla R. Saldivar-Trotter, Federal Bureau of Investigation, hereby certify that a true copy of the foregoing **Remand Comments of Department of Justice and Federal Bureau of Investigation** was served by mail, on this 16th day of November, 2000, to the following parties:

Michael Atschul
Randall S. Coleman
Cellular Telecommunications Industry Association
1250 Connecticut Avenue, N.W.
Washington, D.C. 20036

Matthew J. Flanagan
Telecommunications Industry Association
Suite 300
2500 Wilson Boulevard
Arlington, VA 22201

Jay Kitchen
Personal Communications Industry Association
Suite 700
500 Montgomery Street
Alexandria, VA 22314-1561

Roy Neel
United States Telecom Association
Suite 600
1401 H Street, N.W.
Washington, D.C. 20005-2164

John H. Harwood, II
Lynn R. Charytan
Wilmer, Cutler & Pickering
2445 M Street, N.W.
Washington, D.C. 20037-1420

Theodore B. Olson
Eugene Scalia
Montgomery N. Kosma
Gibson, Dunn & Crutcher LLP
1050 Connecticut Avenue, N.W.
Washington, D.C. 20036-5303

Kurt A. Wimmer
Gerard J. Waldron
Russell D. Jessee
Margaret H. Grebe
Robert A Long, Jr.
Kevin C. Newsom
Covington & Burling
1201 Pennsylvania Avenue, N.W.
Washington, D.C. 20004-2401

Stewart A. Baker
Thomas M. Barba
L. Benjamin Ederington
Matthew L. Stennes
Steptoe & Johnson LLP
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036-1795

_____
Myla R. Saldivar-Trotter