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 REPLY 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 our opening comments, we showed that the Commission's original decision to add the contested punch list capabilities to the J-Standard is fully consistent with CALEA's definition of "call-identifying information" and the cost and privacy criteria of Section 107(b). Although the other commenters attack the punch list capabilities from a variety of angles, they largely repeat arguments that the Commission has already considered and rejected. To the extent that the commenters present new arguments, they fail to come to terms with the language of the statute, the policies underlying it, and the steps that the government has taken to address cost concerns since the initial stages of this proceeding. The Commission therefore should reinstate the punch list capabilities, and in so doing, provide the reasoned explanation that the Court of Appeals found lacking in the Commission's original decision.

DISCUSSION

Perhaps unsurprisingly, most of the comments filed in response to the Commission's latest Public Notice present arguments that have already been aired in earlier rounds of this proceeding. The government has addressed many of those arguments in its prior filings.[1] Rather than repeat ourselves, we will confine our reply comments as far as possible to matters that have not previously been addressed, cross-referencing our earlier filings where appropriate. As we now show, none of the new comments excuses the deficiencies in the J-Standard, and none calls into question the appropriateness of the Commission's original measures to correct those deficiencies.

I. The Meaning of "Call-Identifying Information"

A. General Considerations

---

[1] 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"); DOJ/FBI Remand Comments, CC Docket No. 97-213 (filed November 16, 2000) ("Government Remand Comments").

1. In defending the omission of the punch list capabilities from the J-Standard, a number of commenters assert that only telephone numbers qualify as "call-identifying information." See, e.g., CTIA Comments at 5; USTA Comments at 6; BellSouth Comments at 4. As we have noted before, however, that simply is not what the statute says. CALEA defines "call-identifying information" to mean all "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 language encompasses telephone numbers, but it obviously goes beyond them. If Congress had wished to define "call-identifying information" as (for example) "the numbers dialed or transmitted for the purpose of routing a call" (USTA Comments at 6), it would have said so in the statute. As the D.C. Circuit pointed out, it did not. See USTA v. FCC, 227 F.3d 450, 458 (D.C. Cir. 2000). It was for this reason, among others, that the Court of Appeals affirmed the Commission's determination that wireless location information constitutes "call-identifying information" – a holding that flatly forecloses the commenters' argument that only phone numbers qualify. See id. at 463-464.

The commenters profess to find support from a passage in the legislative history for the argument that "call-identifying information" means telephone numbers. See House Report at 21, reprinted in 1994 USCCAN at 3501. However, we have previously pointed out that this passage does not bear the weight that the commenters place on it. See Second Government Reply Comments at 22-23; USTA, 227 F.3d at 458 (discussing ambiguous

nature of the legislative history). First, the passage draws its language from an earlier version of the legislation, a version that used a different term ("call setup information" rather than "call-identifying information") and defined that term more narrowly than the definition that was ultimately embodied in CALEA. Second, even taken on its own terms, the passage states only that call-identifying information "typically" is information that identifies the numbers dialed or otherwise transmitted for the purpose of routing calls through a carrier's network. House Report at 21, reprinted in 1994 USCCAN at 3501 (emphasis added). The use of the word "typically" makes clear that the House Report's discussion of call-identifying information was not intended to be exhaustive or exclusive. Perhaps for that reason, many of the commenters who quote this passage omit the word "typically" from the quotation. See, e.g., CDT Comments at 6; USTA Comments at 10.

2. In a related vein, several commenters argue that the pen register statute (18 U.S.C. §§ 3121-3127) provides law enforcement only with authority to obtain telephone numbers, and that CALEA's definition of "call-identifying information" should be read in pari materia. See, e.g., BellSouth Comments at 6-7. There are two independent problems with this line of argument.

First, the scope of the pen register statute manifestly is not limited to telephone numbers. The minimization provision of the pen register statute, 18 U.S.C. § 3121(c), which was added by CALEA itself, makes clear that law enforcement is entitled to "record" and "decode" all "electronic or other impulses" that convey "dialing and signaling information

utilized in call processing." This language includes phone numbers, but it is in no way limited to them.

For example, when a person who has "call waiting" service wants to place an existing call on hold and answer an incoming call, he presses a "flash hook" key on his handset that sends a signal to the carrier's switching equipment. The signal tells the switch to complete the circuit between the subject and the incoming caller and to place the existing call on hold. The signal transmitted by the subject's flash hook is not a phone number, but it plainly constitutes "signaling information utilized in call processing." Section 3121(c) makes clear that law enforcement is therefore free to "record" and "decode" it.

Applying the pen register statute to all "dialing and signaling information utilized in call processing," rather than just to phone numbers, is consistent with the statutory and constitutional concerns that underlie federal surveillance law. The use of pen registers to acquire phone numbers is regarded as a negligible intrusion on privacy interests because callers lack a reasonable expectation of privacy in the numbers that they dial to make a call: when they "voluntarily convey[] numerical information to the telephone company and 'expose[]' that information to its equipment in the ordinary course of business," they "assum[e] the risk that the company would reveal" the information to law enforcement. Smith v. Maryland, 442 U.S. 735, 743-744 (1979). The same thing is equally true whenever a caller engages in dialing or signaling activity that is utilized by a carrier in call processing, like pressing a flash hook or signal key to control outgoing and incoming calls. And when the dialing and signaling activity originates with the carrier itself, rather than with the caller

-- for example, when the carrier's switch sends a signal to the subscriber's handset to generate a ringing tone or a busy signal -- the caller's privacy interest in the information is even smaller (indeed, virtually nonexistent), since the caller is not the one sending the signals. See USTA, 227 F.3d at 459 ("Smith's reason for finding no legitimate expectation of privacy in dialed telephone numbers – that callers voluntarily convey this information to the phone company in order to complete calls – applies as well to much of the information provided by the challenged capabilities").

Second, even if the pen register statute were limited to telephone numbers, the pen register statute is only one of a number of different sources of legal authority for electronic surveillance. The most well-known additional source of authority is Title III, which provides law enforcement agencies with authority to intercept the contents of wire and electronic communications. In addition, law enforcement also may obtain surveillance information pursuant to Rule 41 of the Federal Rules of Criminal Procedure (see, e.g., United States v. New York Telephone Co., 434 U.S. 159, 169 (1977); United States v. Falls, 34 F.3d 674, 678-79 (8th Cir. 1994)) and pursuant to 18 U.S.C. § 2703(c), which provides for government access to"record[s] or other information pertaining to a subscriber to or customer of" any provider of wire or electronic communications service. Id. § 2703(c)(1)(A)-(B); see also id. § 2510(15).

There is no indication that Congress intended to limit the definition of "call-identifying information" to the scope of the pen register statute. Indeed, the language of Section 103(a)(2), the provision that requires carriers to be capable of delivering call-

identifying information, points in exactly the opposite direction. Section 103(a)(2) provides that carriers must be able to deliver call-identifying information whenever law enforcement is entitled to obtain such information "pursuant to a court order or other lawful authorization," regardless of whether the source of legal authorization is the pen register statute or some other legal authority. 47 U.S.C. § 1002(a)(2). It also provides that call-identifying information must be provided "in a manner that allows it to be associated with the communication to which it pertains" – a requirement that is directed at Title III surveillance in which law enforcement acquires the underlying contents of the communication as well as the call-identifying information. Finally, Section 103(a)(2) provides that, "with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices * * * , * * * call-identifying information shall not include any information that may disclose the physical location of the subscriber * * * ." This provision presupposes that the definition of "call-identifying information" applies not only to information that is available under the pen register statute, but also – as the Commission has previously recognized in connection with the issue of location information – to information that is available under other sources of legal authority as well. If "call-identifying information" meant nothing more than "information available under the pen register statute," then the location information clause of Section 103(a)(2) would be superfluous. That outcome would conflict with "the well-accepted principle of statutory construction that requires every provision of a statute to be given effect." USTA, 227 F.3d at 463.

3. As noted in our earlier comments, the J-Standard contains its own definition of "call-identifying information," one that purports to define such subsidiary terms as "origin," "direction," "destination," and "termination." In our prior filings, we have explained the shortcomings in this industry-sponsored definition.

CTIA asserts that the Commission is now bound by the J-Standard's definition of "call-identifying information" because no party has previously challenged that definition. CTIA Comments at 2, 8, 12. That assertion is incorrect. The government specifically and explicitly took issue with the J-Standard's definition during the original round of this rulemaking proceeding. See First Government Reply Comments at 30-35. To the extent that the J-Standard definition was inconsistent with the information covered by the punch list capabilities, the Commission's own order effectively superseded the industry definition. Because the Commission's decision granted the government the substantive relief it was seeking, the government obviously had no occasion to ask the Court of Appeals for further "review" of the industry definition.

Nothing in the D.C. Circuit's decision precludes the Commission from explicitly parting company with the J-Standard's definition of "call-identifying information." Rather than holding that the industry definition is binding on the Commission, the D.C. Circuit simply held that the Commission cannot modify the J-Standard "without first identifying its deficiencies." 227 F.3d at 460-461. If the Commission were bound by the J-Standard's definition, there would have been no reason for the Court of Appeals to remand the case, since the J-Standard's definition rules out all of the contested punch list capabilities with the

possible exception of dialed digit extraction. The point of the D.C. Circuit's decision was simply to require the Commission to identify the shortcomings in the J-Standard's definition, not to compel the Commission to accept that definition.

The commenters assert that, even if the J-Standard's definition is not formally binding on the Commission, the industry definition is nevertheless entitled to deference because Congress intended for the Commission to rely on industry expertise. See, e.g., USTA Comments at 4, 7; CTIA Comments at 11. This argument confuses technical expertise with legal expertise. Congress was well aware that industry possessed unique technical knowledge, and the safe-harbor provisions of CALEA reflect Congress's desire to avail itself of that expertise in determining the best means of meeting CALEA's legal requirements. But technical expertise in figuring out how to implement legal requirements is very different from legal expertise in determining what the legal requirements are. Industry hardly can claim to have unique legal expertise regarding the meaning of CALEA, and nothing in CALEA itself suggests in the slightest that Congress intended for industry's self-interested views of the law to be given deference. To the contrary, the whole point of Section 107(b) is to place disputes about the legal sufficiency of industry standards in the hands of an administrative agency with the requisite impartiality and legal expertise to resolve such disputes. The Third Report and Order properly reflected this distinction between legal and technical expertise: the Commission decided what the law required, then invited industry to revise the technical standards to implement the legal requirements in a technically sound manner. See Third Report and Order ¶¶ 124-129. For the Commission to "defer" to industry's legal views,

rather than to its technical expertise, would be to abdicate the role that Congress assigned the Commission under Section 107(b). Cf. USTA, 227 F.3d at 459 ("the authors of the J-Standard can provide no guidance" on whether Congress clearly intended to limit "call-identifying information" to phone numbers).[2]

4. Section 103(a)(2) of CALEA requires carriers to have the capability to deliver "reasonably available" call-identifying information. A few commenters assert that one or more of the punch list capabilities involve information that is not "reasonably available" and therefore is outside the scope of CALEA. See, e.g., PCIA Comments at 9; BellSouth Comments at 8-9.

As explained in our earlier filings, the question whether a particular kind of call-identifying information is "reasonably available" does not lend itself to across-the-board, industry-wide answers. See Second Government Comments at 18-20. Industry itself recognized this fact when it was framing the J-Standard, pointing out that "[t]he specific elements of call-identifying information that are reasonably available at an IAP may vary between different technologies and may change as technology evolves." J-STD-025 § 4.2.1.

---

[2] Mysteriously, USTA asserts that the J-Standard "represents a consensus of industry and law enforcement experts." USTA Comments at 5. Although industry and law enforcement reached a consensus on a number of points, there was a manifest lack of consensus between industry and law enforcement on several important issues. It was that very lack of consensus that gave rise to this proceeding.

Accordingly, the J-Standard made no attempt to determine what information was or was not "reasonably available." Instead, the J-Standard adopted a general definition of "reasonably available" and left the application of that definition to be carried out on a case-by-case basis. For its part, the Commission modified the J-Standard's general definition of "reasonably available" (see Third Report and Order ¶ 28), but adhered to industry's approach of leaving disputes over reasonable availability to be resolved on a case-by-case basis.

The commenters who are now raising reasonable availability issues have failed to come to terms with this basic approach – an approach, it must be underscored, that was adopted by industry itself in the J-Standard. The commenters are asking the Commission to make a global determination that (for example) party join/hold/drop information is not "reasonably available" because of asserted technical burdens involved in making the information available to law enforcement. See BellSouth Comments at 15. Such a determination would remove the punch list capabilities from the J-Standard with respect to every switch platform, past, present, and future, regardless of potential differences among switches and network architectures. Neither the Third Report and Order nor the J-Standard itself countenances this kind of blunderbuss approach, and there is no reason to adopt such an approach now.

Moreover, as a factual matter, the asserted burdens involved in providing the contested punch list capabilities are vastly overstated. As explained in our opening comments, manufacturers such as Lucent, Nortel, and Siemens, whose switches account for 85 percent of the market, have already entered into cooperative agreements to implement the

J-Standard and the punch list capabilities on their switch platforms. In so doing, the switch manufacturers – who, unlike carriers, are actually responsible for designing CALEA solutions – have made clear that there are no serious technical obstacles to implementing the punch list capabilities.

B. Dialed Digit Extraction

1. Many commenters argue that post-cut-through dialed digits do not constitute call-identifying information "from the perspective of" the originating carrier, because the originating carrier (in contrast to an IXC or other downstream carriers) does not use the information to route the call. See, e.g., CDT Comments at 6; CTIA Comments at 13; USTA Comments at 9; Verizon Comments at 4. We have addressed this argument in our earlier filings. As we have explained at length, nowhere does the definition of "call-identifying information" ask which carrier uses the information for call routing purposes. More generally, dialing and signaling information does not transform itself from call-identifying information to something else (or vice versa) as it passes through the PSTN. If the information identifies the "origin, direction, destination, or termination" of a "communication," then it fits squarely within CALEA's definition of "call-identifying information," regardless of how a particular carrier handles it. See Second Government Reply Comments at 23-26. There is simply no room in the statutory definition for the commenters' approach.[3]

[3] For this reason, it is immaterial that wireless switches, in contrast to wireline switches, do not use DTMF tones for call routing purposes. See Cingular Comments at 6. When a

Moreover, to hold that dialing and signaling information is not call-identifying information if a particular carrier does not use the information for call routing purposes would mean that, in many cases, even telephone numbers would not qualify as call-identifying information. As we have noted before, when a subscriber dials a conventional inter-LATA long-distance call (e.g., "1-918-123-4567"), the subscriber's LEC uses only the area code ("918") to route the call; it does nothing with the remainder of the phone number ("123-4567") other than pass it along to the subscriber's IXC. Under the commenters' view of CALEA, only the area code would qualify as call-identifying information "from the perspective of" the LEC, and hence the LEC would be under no obligation to provide law enforcement with access to the rest of the called party's telephone number. See Government Remand Comments at 22 n.1. Needless to say, CALEA can hardly be construed in a way that leads to such a preposterous result.

2. CTIA suggests that post-cut-through dialed digits should not be regarded as "call-identifying information" because to do so would be to expand law enforcement's surveillance capabilities beyond their traditional scope. CTIA Comments at 13. But as we have explained previously, law enforcement has always had the capability to obtain dialed digits, post-cut-through as well as pre-cut-through, in the POTS environment. See Second

---

subject dials post-cut-through digits to complete a call, those digits represent call-identifying information regardless of whether the originating carrier uses (or is able to use) the digits to route the call.

Government Reply Comments, Declaration of Supervisory Special Agent Dave Yarbrough ¶¶ 48-50 (1/27/99). The methods of obtaining dialed digits have varied depending on whether a wireline or wireless communication is being monitored, but the ultimate capacity to obtain the digits has always been present. As a result, adding dialed digit extraction to the J-Standard will not result in an expansion of law enforcement's traditional surveillance capabilities.

C. The Other Punch List Capabilities

1. Subject-Initiated Dialing and Signaling

BellSouth asserts that a subject's use of a flash hook or feature keys does not result in call-identifying information because the use of such keys "ha[s] nothing to do with the routing of a call." BellSouth Comments at 16. That is manifestly incorrect. When a subject presses a flash hook or a feature key to utilize (for example) call transfer or call waiting, the resulting signals are transmitted to the carrier's switch precisely so the switch can control the various legs of the call and route the communication properly. It is nonsensical to suggest that such dialing and signaling activity is unrelated to call routing.

BellSouth also asserts that "similar" information is already provided to law enforcement under the J-Standard. BellSouth Comments at 17. We have addressed this argument at length in our earlier filings. See First Government Comments at 48-49; First Government Reply Comments at 49-50; Second Government Reply Comments at 46. As we have explained there, the messages provided by the J-Standard do not capture all of the call-identifying information that is generated when a subject engages in dialing and signaling

activity to control his calls. Although there may be specific instances in which a particular subject-initiated dialing or signaling action can be detected or inferred through the messages provided by the J-Standard, that will often not be the case, and law enforcement's inability to follow the course of the subject's dialing and signaling activities can have serious adverse consequences for a criminal investigation.

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

Several commenters argue that in-band and out-of-band network signaling does not constitute call-identifying information because the signals in question, such as busy signals, are often generated during unsuccessful call attempts and therefore do not involve "communications." See USTA Comments at 9; CTIA Comments at 17; BellSouth Comments at 18. The suggestion that no "communication" exists for CALEA purposes until and unless the call is completed is a preposterous one. Under the J-Standard itself, a TerminationAttempt message is sent to law enforcement to report every "incoming circuit-mode call attempt to the intercept subject," and the message is delivered "regardless of the disposition of the call (e.g., busy, answered, [or] redirected"). J-STD-025 § 5.4.10 (emphasis added). Industry thus recognizes that CALEA is intended to provide law enforcement with access to call-identifying information relating to unsuccessful as well as successful call attempts. If the definition of "call-identifying information" were construed to exclude unsuccessful call attempts, then law enforcement would be denied access even to the telephone numbers associated with such call attempts – a result that is directly contrary to

law enforcement's traditional surveillance capabilities and that cannot possibly be claimed to be consistent with Congress's goals in enacting CALEA.

USTA and BellSouth also assert that the J-Standard already provides law enforcement with the same information that would be provided by this punch list capability. See USTA Comments at 9; BellSouth Comments at 19. We have addressed this argument at length before, explaining why the J-Standard's existing message set does not duplicate the network signaling information sought by law enforcement in this proceeding, and we refer the Commission to our earlier discussion. See Government Reply Comments at 57-59.

Finally, BellSouth asserts that network signaling is not "reasonably available" because a carrier would have to install new equipment at its local switch to detect tones and signals returned over a connection to a remote switch, such as a busy signal generated by an IXE's switch. See BellSouth Comments at 19. Law enforcement has never claimed that a carrier must be capable of providing network signals that originate in another carrier's network, and nothing in the Commission's original decision requires delivery of such signals. See Third Report and Order ¶ 89. As for signals that originate elsewhere in the carrier's own network and are transmitted through the IAP toward the intercept subject, the Commission found that such signals can be made available "without excessive modifications to the network" (ibid.), and BellSouth's submission, which simply asserts that network modifications would be required to implement this capability, does not prove otherwise.

3. Party Join/Hold/Drop Information

In arguing that party join/hold/drop information is not "call-identifying information," the commenters rely primarily on the theory that call-identifying information does not include information about changes in the various legs of a multi-party call. See, e.g., CDT Comments at 9; USTA Comments at 7-8. As we have explained repeatedly before, however, CALEA's definition of "call-identifying information" covers all dialing and signaling information that identifies the origin, direction, destination, or termination of "each communication generated or received by a subscriber." 42 U.S.C. § 1001(2) (emphasis added). A multi-leg call can, and often does, involve more than one "communication" – for example, when one party toggles back and forth between two other parties, speaking first to one and then to the other. As a result, a carrier must be capable of notifying law enforcement about changes in party status (such as "party join" or "party drop") that affect the path of the subsequent communications. The J-Standard's Change message reports only changes in "call identity," and because the Change message does not require a separate call identity for each leg of a multi-leg call, it is not a substitute for party join/hold/drop information. See First Government Reply Comments at 48-49, 51.[4]

[4] BellSouth asserts that other messages, such as the TerminationAttempt and Origination messages, also provide the party status information sought by law enforcement. See BellSouth 15-16. That suggestion is likewise incorrect. See First Government Reply Comments at 51-52.

CTIA suggests that party join/hold/drop information is superfluous in Title III cases because law enforcement can determine the parties to a multi-leg call simply by listening to their voices. CTIA Comments at 16. But there are any number of situations in which this suggestion falls short – for example, when parties are listening without speaking, or when two parties have sufficiently similar voices to raise a reasonable doubt in the mind of a jury. When a criminal defendant asserts that he dropped off a critical multi-party call before the incriminating exchange, law enforcement may be entirely unable to confirm or rebut his testimony in the absence of party join/hold/drop information.[5]

II. Cost Considerations

A. In General

In our opening comments, we made two basic points regarding the application of Section 107(b)'s cost criteria to the four contested punch list capabilities. The first point is that the implementation of these capabilities will impose relatively few costs on carriers and their customers – partly because the costs associated with these capabilities are small and partly because the government will wind up bearing the lion's share of the costs that are

[5] CTIA also suggests that party join/hold/drop is relevant only in Title III cases, not when law enforcement is proceeding under the pen register statute. That too is incorrect. For example, if law enforcement can obtain information through a pen register about which parties were "on the call" at which times, the information may help to corroborate (or contradict) information provided by an informant or other sources.

incurred. The second point is that there are no less expensive alternatives that meet the assistance capability requirements of CALEA. As a result, the punch list capabilities satisfy the cost requirements of Section 107(b): they represent "cost-effective methods" of meeting CALEA's assistance capability requirements and they "minimize the cost of such compliance on residential ratepayers."

Several of the commenters forthrightly admit that the steps taken by the government to implement CALEA, such as the granting of right-to-use licenses for CALEA software solutions and the development of the flexible deployment program, have substantially diminished the cost concerns that were aired in earlier stages of this proceeding. CTIA acknowledges that "[t]he cost recovery landscape certainly has changed" since the time of the Commission's original decision, and USTA acknowledges that "[t]hese actions [by the government] provide carriers and manufacturers with the ability to implement CALEA by cost-effective methods." USTA Comments at 13.

In contrast, BellSouth asserts that it expects to incur costs ranging from $193 million to $286 million to implement the six punch list capabilities covered by the Third Report and Order. BellSouth Comments at 21-22. BellSouth offers no substantiation for these figures, and we submit that without substantiation, they simply are not credible. BellSouth claims that its estimates are based on "general data obtained from vendors" (id. at 21), yet like all other carriers, BellSouth will pay nothing for the software required to implement CALEA on Lucent, Nortel, Siemens, and AGCS switching platforms. Moreover, BellSouth has applied for a deadline extension pursuant to the government's flexible deployment program,

which would permit it to adhere to its usual software upgrade cycle, and like other carriers, it is eligible for federal reimbursement for costs attributable to CALEA's capacity requirements. BellSouth offers no explanation of how it could wind up paying several hundred million dollars even after these cost-shifting and cost-minimizing measures are taken into account. Tellingly, no other carrier has advanced similar cost claims.[6]

USTA observes that the government's cooperative agreements and flexible deployment program "do not defray all of the costs of CALEA." USTA Comments at 13. That is undoubtedly correct. But nowhere did Congress suggest that the costs of CALEA were to be borne exclusively by the federal government. Section 107(b) calls on the

---

[6] USTA asserts that the cost of meeting CALEA's capacity requirements (as distinct from CALEA's capability requirements) "could range from approximately $2.35 per line to $3.66 per line." USTA Comments at 13 n.8. USTA provides no explanation of how it derived these cost estimates. Absent some such explanation, the bare numbers themselves can hardly be given weight. In any event, as explained in our opening comments, capacity costs are generally the responsibility of the government, and carriers who have filed timely capacity statements are eligible for reimbursement. 47 U.S.C. § 1003(d)-(e); see Government Remand Comments at 33-35. As a result, CALEA's capacity requirements manifestly will not result in a per-line cost of $2.35, $3.66, or any remotely comparable number. And apart from dialed digit extraction, none of the contested punch list items has any potential to produce additional capacity costs.

Commission to employ cost-effective methods of meeting CALEA's assistance capability requirements – not to hold carriers harmless from any conceivable financial burden. Moreover, the costs that matter here are those specifically attributable to the four contested punch list capabilities, not the sum total of all possible CALEA implementation costs.

USTA also asserts that the costs incurred by carriers under CALEA "are solely for the benefit of law enforcement." USTA Comments at 13. With due respect, that is a remarkably narrow view of the matter. When a federal, state, or local law enforcement agency engages in lawful electronic surveillance, it is seeking to protect the public from serious and often violent criminal activities. The assistance capability requirements of CALEA inure to the benefit of everyone, not simply to law enforcement.

Finally, CTIA suggests that the Commission must weigh the impact of its decision on competition in the telecommunications industry. CTIA Comments at 23 & n.70. We see no statutory basis for that suggestion.[7] In any event, CTIA's stated competitive concerns involve reimbursement issues before the Department of Justice, not the standard-setting issues now before the Commission. Because the government's cooperative agreements cover the vast majority of wireline and wireless switches currently in use, there is no reason to think that

[7] The criteria that govern this proceeding are those set forth in Section 107(b), and none of the criteria in Section 107(b) refers to competition. The provision on which CTIA relies, 47 U.S.C. § 160, is directed at the Commission's exercise of its powers under the Communications Act of 1934, not at the separate and distinct powers conferred on the Commission by CALEA.

the Commission's disposition of this proceeding will have a material effect on industrywide competition.

B. Dialed Digit Extraction

The only individual punch list capability whose costs have attracted significant comments is dialed digit extraction. The commenters note that hardware resources such as tone decoders may be required to implement dialed digit extraction. They argue that the need to use such hardware may result in additional costs beyond those attributable to the software component of the CALEA solution – costs which they characterize as "enormous" and "staggering" (AT&T Comments at 11-12).

In large part, these cost concerns appear to overlook the distinction between the assistance capability requirements of Section 103 and the assistance capacity requirements of Section 104. To the extent that additional hardware is required to meet CALEA's capacity requirements, carriers are eligible to seek reimbursement under Section 104 of CALEA. See Government Remand Comments at 33-34. For example, in explaining why it regards the costs of dialed digit extraction as "enormous," AT&T suggests that "hundreds of thousands of lines * * * may need to be tapped simultaneously under the FBI's capacity notice." AT&T Comments at 11; see also PCIA Comments at 9-10. Even if that figure were correct, it would not follow that the capacity costs associated with providing dialed digit extraction for "hundreds of thousands of lines" would be borne by the carriers. Instead, to the extent that a carrier is required to add tone decoders or other hardware to a switch to meet the capacity

requirements of Section 104, the carrier is eligible to seek reimbursement under Section 104(e) and the government's cost-recovery regulations.[8]

[8] USTA and BellSouth assert that, because tone decoders are treated as shared resources in wireline switches, the implementation of dialed digit extraction could adversely affect network availability by tying up tone decoders that would otherwise be available for customer service purposes. USTA 10-11; BellSouth Comments at 13. If a particular switch will not have the capacity to perform dialed digit extraction without degrading call processing capabilities, the carrier can add hardware resources to enable the switch to carry out both functions concurrently. As explained, to the extent that additional hardware costs are required by CALEA's capacity requirements, the carrier can seek reimbursement from the government for such costs.

AT&T suggests that it would be less expensive for originating carriers to deliver post-cut-through digits to law enforcement on a call content channel and to have law enforcement agencies use their own tone decoders to extract dialed digits from the channel. AT&T Comments at 12; see also PCIA Comments at 10. As a threshold matter, it is by no means obvious that this alternative would be less expensive than dialed digit extraction in the long run: as explained in our earlier filings, the cost of provisioning pen register intercepts to accommodate the delivery of post-cut-through content over a call content channel could amount to as much as $20 million per year, year in and year out. See Second Government Reply Comments at 63-64. But in any event, AT&T's solution raises privacy issues that are not presented by dialed digit extraction. With dialed digit extraction, law enforcement receives only post-cut-through digits, not audio signals and other post-cut-through content. Under AT&T's approach, in contrast, law enforcement would receive all of the content of the call. As between these two alternatives, dialed digit extraction is surely more consistent with the privacy concerns of CALEA.[9]

[9] USTA suggests that a decision by the Commission to add dialed digit extraction to the

J-Standard would conflict with Section 103(b)(1)(A) of CALEA, which provides that "[t]his subchapter does not authorize any law enforcement agency or officer * * * to require any specific design of equipment, facilities, services, features, or system configurations * * * ." 42 U.S.C. § 103(b)(1)(A). There are two problems with that argument. First, by its terms, Section 103(b)(1)(A) is directed solely at "law enforcement agenc[ies]," not at the Commission. Second, and more important, dialed digit extraction does not entail or dictate "any specific design of equipment, facilities, services, features, or system configurations" (emphasis added). Dialed digit extraction is merely a capability; the specific software and/or hardware design used to implement the capability is up to the manufacturer and may vary from switch to switch.

III. Privacy Considerations

The only punch list capability with respect to which serious privacy questions have been raised is dialed digit extraction. In our opening comments, we showed that the use of dialed digit extraction to deliver post-cut-through dialed digits is consistent with Section 107(b)(2) of CALEA, which calls on the Commission to establish standards that "protect the privacy and security of communications not authorized to be intercepted." See Government Remand Comments at 47-51. We also showed that the alternatives to dialed digit extraction that have previously been advanced by other commenters, such as requiring law enforcement to obtain a Title III intercept order or to seek post-cut-through digits after the fact from the IXE, do not "meet the assistance requirements" of CALEA (47 U.S.C. § 1006(b)(1)) because they do not "ensure" that law enforcement can obtain the information at all, much less that the information can be obtained "before, during, or immediately after" the communication (id. § 1002(a)(2)). Although the other commenters renew their privacy objections to dialed digit extraction, they have not overcome these points.

A. The Legal Standards Governing Dialed Digit Extraction

As explained in our earlier comments, when Congress enacted CALEA, it was well aware that law enforcement traditionally had obtained post-cut-through dialed digits in pen register cases. Its solution was not to place post-cut-through digits outside the scope of the pen register statute, nor was it to require a heightened evidentiary showing for the delivery of such information. Instead, Congress enacted 18 U.S.C. § 3121(c), the pen register statute's minimization provision, which directs law enforcement to use "reasonably available" technology to "restrict[] the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing." Section 3121(c) reflects Congress's awareness that law enforcement receives post-cut-through digits in pen register cases, and it presupposes that the delivery of post-cut-through digits to law enforcement is within the scope of the authority provided by the pen register statute.

CTIA suggests that it is paradoxical for the government to require carriers to deliver post-cut-through digits at the same time that Section 3121(c) obligates law enforcement (in CTIA's words) "to use additional technology to avoid receiving them." CTIA Comments at 20. This supposed paradox is due solely to CTIA's misunderstanding of Section 3121(c). Section 3121(c) manifestly does not obligate law enforcement to "avoid receiving" post-cut-through digits under a pen register order. Instead, it simply obligates law enforcement to use reasonably available technology (if any exists) to avoid "recording and decoding" post-cut-through digits and other signals that are not "utilized in call processing." Nothing

in Section 3121(c) precludes the government from recording and decoding post-cut-through digits that are "utilized in call processing" -- quite the contrary.

CTIA claims that Section 3121(c) was intended not to regulate the treatment of post-cut-through digits, but rather to adopt the state-law decision of the New York Court of Appeals in People v. Bialostok, 80 N.Y.2d 738, 610 N.E.2d 374 (1993). Bialostok holds that "a pen register having the additional capability to monitor conversations should be treated as an eavesdropping device under the [New York] Criminal Procedure Law and therefore [should be] permitted only when a magistrate has issued a warrant based on probable cause." 80 N.Y.2d at 742, 610 N.E.2d at 376. Unfortunately for CTIA, nothing in the language of Section 3121(c) even remotely suggests that Congress intended to federalize this state-law rule. Section 3121(c) does not make any reference to pen registers that are capable of "monitor[ing] conversations," much less impose a warrant requirement on such devices. And nothing in the legislative history of CALEA suggests in any way that Section 3121(c) was meant to incorporate the Bialostok rule. The passage from the House Report that is quoted by CTIA, far from supporting CTIA's argument, cuts the other way: it makes no reference either to Bialostok or to the warrant requirement, and it makes clear that Congress was speaking instead about the development of technology that could distinguish between "call processing" digits and "content" digits. See House Report at 32, reprinted in 1994 USCCAN at 3512. To our knowledge, no case has ever held that New York's Bialostok rule applies to

the federal pen register statute, whether by virtue of Section 3121(c) or any other provision of the statute, and CTIA cites no such case.[10]

Turning from Section 3121(c) to the case law, several commenters suggest that the Fourth Circuit's decision in Brown v. Waddell, 50 F.3d 285 (1995), precludes law enforcement from obtaining post-cut-through dialed digits on the basis of a pen register order. See, e.g., CDT Comments at 6; AT&T Comments at 7-8. However, nothing in Brown supports that argument. Brown holds that "clone pagers," which are used by law enforcement to intercept messages transmitted to digital display pagers, do not constitute pen registers and are subject instead to the requirements of Title III. 50 F.3d at 289-94. That holding is an unremarkable one, because digital display pagers are used exclusively to "'display visual messages'" from a calling party, whether in the form of numbers or words. See id. at 291 (quoting S. Rep. No. 541, 99th Cong., 2d Sess. 9-10 (1986), reprinted in 1986 USCCAN 3555, 3563-64). The whole point of using a clone pager is to obtain the content of those messages. Even on those occasions when the message that the calling party chooses to transmit is a telephone number (typically, but not necessarily, his own), the numbers are entered and transmitted solely to provide information to the pager customer, not for call

[10] Indeed, even New York itself no longer follows the Bialostok rule. See People v. Martello, 93 N.Y.2d 645, 654 (1999) (current New York law "evinces a legislative intent to view all pen registers, including those readily adaptable as eavesdropping devices, as pen registers and not, as Bialostok held, as eavesdropping devices").

processing purposes. Nothing in Brown suggests that a conventional pen register device is somehow transformed into the legal equivalent of a clone pager simply because some of the numbers that it records may, in particular cases, be transmitted for purposes other than call completion, and no court has ever so held.

Several commenters also suggest that the decision of the Court of Appeals in this very case precludes the delivery of post-cut-through digits to law enforcement on the basis of a pen register order. They ground this surprising suggestion not in the D.C. Circuit's discussion of dialed digit extraction, which says nothing of the kind, but rather in the court's discussion of packet-mode surveillance issues. The commenters read the court's opinion to hold that carriers may not deliver full packets – packets containing content as well as routing information – without a Title III order. See CDT Comments at 12-13; CTIA Comments at 19-20; Cisco Comments at 6-7. They reason that if the delivery of full packets requires a Title III order because packets may contain content, then dialed digit extraction must likewise require a Title III order because post-cut-through digits may (in some instances) be content as well.

The problem with this argument is that it rests on a misreading of the D.C. Circuit's decision. In discussing the J-Standard's provisions regarding the delivery of packet-mode data, the court stated:

> [N]othing in the Commission's treatment of packet-mode data requires carriers to turn over call content to law enforcement agencies absent lawful authorization. Although the Commission appears to have interpreted the J-Standard as expanding the authority of law enforcement agencies to obtain the contents of communications, see id., the Commission was simply mistaken.

> All of CALEA's required capabilities are expressly premised on the condition that any information will be obtained "pursuant to a court order or other lawful authorization." 47 U.S.C. § 1002(a)(1)-(3). CALEA authorizes neither the Commission nor the telecommunications industry to modify either the evidentiary standards or procedural safeguards for securing legal authorization to obtain packets from which call content has not been stripped, nor may the Commission require carriers to provide the government with information that is "not authorized to be intercepted." Id. See also Final Brief for the United States at 4 ("If the government lacks the requisite legal authority to obtain particular information, nothing in Section 103 obligates a carrier to provide such information."). Petitioners thus have no reason to fear that "compliance with the Order will force carriers to violate their duty under CALEA to 'protect the privacy and security of communications ... not authorized to be intercepted.'" Final Brief of Petitioners USTA, CTIA, and CDT at 35.

This passage makes a simple point – namely, that neither CALEA itself nor the Commission's order requires (or can require) carriers to deliver the content portion of a packet data stream in the absence of "legal authorization." What the passage does not do is to specify what the requisite "legal authorization" is. Instead, it simply says that the governing legal authority – whatever it may be – is not affected or countermanded by CALEA or the Commission's order. That holding, while important for purposes of the court's decision, casts no light on the question at hand.

Finally, CDT suggests in passing that the delivery of post-cut-through digits on the basis of a pen register order offends the Fourth Amendment. CDT Comments at 6. That suggestion is equally incorrect. When a law enforcement agency has legal authority to engage in electronic surveillance and is acting within the scope of its authority, the Fourth Amendment is not violated simply because the agency comes across information in the course of the surveillance that it would not otherwise be independently entitled to acquire.

Cf. United States v. Williams, 822 F.2d 1174, 1182 (D.C. Cir.1987) ("apprehension of that which is already in plain view of an officer lawfully present at his vantage point" does not constitute Fourth Amendment search). Thus, if a law enforcement agency has authority under the pen register statute to capture post-cut-through digits used for call completion purposes, the bare fact that it may (unavoidably) see digits entered for other purposes does not offend the Fourth Amendment. The intrusion on privacy interests is particularly modest because, without further information, dialed digits themselves disclose virtually nothing intelligible about a subject's transactional activities.

B. Alternatives To Dialed Digit Extraction

The commenters offer two principal alternatives to dialed digit extraction: obtaining post-cut-through digits from the originating carrier pursuant to a Title III order or serving a pen register order on the downstream carrier (e.g., the IXE) that uses the post-cut-through digits for call completion purposes. We have explained the deficiencies with these alternatives in the past, and we will not repeat that explanation here. See Government Remand Comments at 52-55. What we wish to emphasize is that we are not objecting to these alternatives simply because they are "less convenient or more costly" (BellSouth Comments at 11). Instead, we object to them because they do not meet the requirements of CALEA itself. Section 103(a)(2) of CALEA requires every carrier to be capable of delivering all reasonably available call-identifying information to law enforcement and of doing so contemporaneously with the transmission of the underlying communication. For reasons that we have given previously, if law enforcement were remitted to the alternatives proposed by

the commenters, it would not obtain all of the post-cut-through digits that it is legally entitled to obtain, and even when it did, it would not obtain them in the timely manner required by CALEA. What is at issue is not whether law enforcement is entitled to "one-stop shopping," but whether the assistance capability requirements of Section 103 will be met or not.

IV. Other Matters

One commenter, Cisco Systems, has submitted extensive comments regarding the proper implementation of CALEA and the J-Standard for packet-mode communications. These comments are wholly outside the scope of the Commission's Public Notice, and the government therefore will not address the subject of packet-mode communications here. If the Commission calls for public comments regarding packet-mode issues in connection with its consideration of TIA's "JEM" (Joint Experts Meeting) report, the government will submit comments at that time.

DATE: December 8, 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

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

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

CERTIFICATE OF SERVICE

Scott R. McIntosh, Special Counsel, Appellate Staff, Civil Division, Department of Justice, hereby certifies that the foregoing REMAND REPLY COMMENTS OF DEPARTMENT OF JUSTICE AND FEDERAL BUREAU OF INVESTIGATION was served on December 8, 2000, by mailing copies by first-class mail to the persons on the attached service list.

/s/
Scott R. McIntosh

SERVICE LIST

Rodney Small
Office of Engineering & Technology
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Julius Knapp
Office of Engineering & Technology
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Geraldine Matise
Office of Engineering & Technology
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

James X. Dempsey, Senior Staff Counsel
Center for Democracy and Technology
1634 Eye Street, N.W., Suite 1100
Washington, D.C. 20006
(202)637-9800

Scott Blake Harris
Kelly S. McGinn
Harris, Wilshire & Grannis LLP
1200 Eighteenth Street, N.W.
Washington, D.C. 20036
(202)730-1300 office
(202)730-1301 fax

Hope Thurrott
Roger K. Toppins
Paul Mancini
SBC Communications, Inc.
1401 I Street NW, 11th Floor
Washington, D.C. 20005
(202)326-8891

Lawrence E. Sarjeant
Linda L. Kent
Keith Townsend
John W. Hunter
Julie E. Rones
United States Telecom Association
1401 H Street, N.W. Suite 600
Washington, D.C. 20005

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

Joaquin R. Carbonell
Carol L. Tacker
Cingular Wireless LLC
1100 Peachtree Street, N.E, Suite 910
Atlanta, GA 30309
(404)249-0917

M. Robert Sutherland
Angela N. Brown
Bell South Corporation
Suite 1700 - 1155 Peachtree Street, N.E.
Atlanta, GA 30309-3610
(404)249-3392

J. Lloyd Nault, II
Bell South Telecommunications, Inc.
Suite 1700 - 1155 Peachtree Street, N.E.
Atlanta, GA 30309-3610
(404)249-2604

Sylvia Lesse
John Kuykendall
KRASKIN, LESSE & COSSON, LLP
21201 I.. Street, N.W.
Suite 520
Washington, D.C. 20037
(202)296-8890

Grant Seifert, Vice President
Government Relations
Matthew J. Flanigan, President
Telecommunications Industry Association
1300 Pennsylvania Avenue, N.W.
Suite 350
Washington, D.C. 20004
(202)383-1483

Robert L. Hoggarth, Senior Vice President
Government Relations
Donald Vasek, Director
Government Relations
Personal Communications Industry Association
500 Montgomery Street, Suite 700
Alexandria, VA 22314
(703)739-0300

Stewart A. Baker
Thomas M. Barbe
Todd B. Lantor
Steptoe & Johnson, LLP
1330 Connecticut Ave., N.W.
Washington, D.C. 20036
(202)429-3000

Mark C. Rosenblum
Stephen C. Garavito
Martha Lewis Marcus
AT&T Corp.
Room 1131M1
295 North Maple Avenue
Basking Ridge, New Jersey 07920
(908)221-8100

Roseanna DeMaria
AT&T Wireless Group
Room N812A
32 Avenue of the Americas
New York, New York 10013
(212)830-6364

John M. Goodman
1300 I. Street, N.W.
Washington, D.C. 20005
(202)336-7874

Michael Atschul
Randall S. Coleman
Cellular Telecommunications Industry Association
1250 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20036

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
Gerad 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