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

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

REPLY COMMENTS REGARDING
FURTHER NOTICE OF PROPOSED RULEMAKING

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

Donald Remy
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 response to the Commission's Further Notice of Proposed Rulemaking, the parties who oppose the government's rulemaking petition have raised a host of objections to the Commission's tentative conclusions about the assistance capabilities at issue in this proceeding. The commenters variously argue that the capabilities tentatively approved by the Commission are not required by CALEA; that they are technically infeasible; that they are ruinously expensive; and that, if they are nevertheless adopted by the Commission, they cannot be implemented without protracted delay.

In the main, these arguments are not new. Instead, they simply repeat and elaborate on the arguments that the commenters made in earlier rounds of this rulemaking. The Commission rightly found those arguments unpersuasive when it issued the Further Notice of Proposed Rulemaking, and nothing that the commenters have said in the latest round of comments provides any reason for the Commission to revise that judgment.

Although the commenters attack the Commission's tentative conclusions from a variety of different angles, their arguments have one thing in common: a fundamental unwillingness to acknowledge the law enforcement interests at stake in this proceeding. As we have explained before, the ability to carry out legally authorized electronic surveillance is vital to the efforts of federal, state, and local law enforcement agencies to protect the public by detecting, preventing, and prosecuting criminal activity. The underlying purpose of CALEA was to close the growing gap between law enforcement's legal authority to conduct electronic surveillance and its technical ability to carry out that authority. Yet, if the J-Standard is not modified to include the assistance capabilities at issue in this proceeding, law enforcement inevitably will be denied information about criminal activity to

which it is legally entitled and which it needs to protect public safety and security. The commenters have averted their eyes to this outcome; the Commission must not.

As part of this filing, we are submitting declarations by the Director of the Federal Bureau of Investigation and the Administrator of the Drug Enforcement Administration that attest to the vital law enforcement interests at stake in this proceeding. It is imperative for the Commission to keep these interests firmly in mind -- not simply because they are intrinsically important, but because they are the interests that led Congress to enact CALEA in the first place. By following through on the changes proposed in the Further Notice of Proposed Rulemaking, the Commission will be vindicating Congress's underlying goals, and discharging the Commission's own responsibilities under CALEA, at the same time that it is protecting the public interest in effective law enforcement.

DISCUSSION

Introduction

The Department of Justice and the Federal Bureau of Investigation submit these reply comments pursuant to the Commission's Further Notice of Proposed Rulemaking (Notice) in this proceeding. These reply comments are submitted in response to the comments filed by other parties on December 14, 1998, concerning the tentative conclusions and questions set forth by the Commission in its Notice.

Perhaps unsurprisingly, the latest round of comments from industry and other commenters bears a strong resemblance to the comments filed by the same parties in May 1998 and June 1998, in response to the Commission's initial public notice. To the extent that the latest set of filings merely repeats prior comments, we have attempted to avoid repeating our own prior remarks unnecessarily. Instead, where possible, we have identified the relevant portions of our earlier filings and refer the Commission to the referenced materials for a more complete explanation of our position.

The comments that follow are divided into three parts. In Part I, we reply to general comments from other parties concerning Section 103(a) of CALEA, which prescribes electronic surveillance assistance capability requirements for telecommunications carriers, and Section 107(b) of CALEA, which prescribes the Commission's role in identifying and correcting deficiencies in industry "safe harbor" technical standards. Among other things, we address the general policies that underlie CALEA, the role of cost considerations in this proceeding, and the general scope of the carriers' obligation to provide law enforcement with reasonably available call-identifying information. The issues discussed in Part I are germane to each of the individual assistance capabilities at issue in this proceeding.

In Part II, we reply to comments concerning the individual assistance capabilities at issue in this proceeding. We address both the assistance capabilities that the government is seeking to add to J-STD-025 (the "J-Standard") and the existing capabilities in the J-Standard that CDT and other privacy groups are seeking to restrict. Finally, in Part III, we reply to comments concerning the implementation of the Commission's forthcoming order. In particular, we address issues relating to the proposed "remand" to TIA and the deadline for implementing the assistance capability requirements established in this proceeding.

In conjunction with these reply comments, we are submitting declarations of Louis J. Freeh, Director of the Federal Bureau of Investigations, and Thomas A. Constantine, Administrator of the Drug Enforcement Administration. FBI Director Freeh and DEA Administrator Constantine address the issues before the Commission from the perspective of the federal government's most senior law enforcement officials. They explain not only the general importance of electronic surveillance to law enforcement, but also law enforcement's particular need for the assistance capabilities at issue in this proceeding. See, e.g., Freeh Dec. ¶¶21(A)-21(H). These declarations answer the recurring suggestion by other commenters that the capabilities being sought in this proceeding are relatively inconsequential for law enforcement -- mere "dessert," as one commenter puts it (CTIA Comments at 5).

We also present a declaration by FBI Supervisory Special Agent Dave Yarbrough. Mr. Yarbrough's declaration discusses the assistance capability issues in this proceeding from the perspective of a law enforcement agent who has extensive personal experience in legally authorized electronic surveillance. Mr. Yarbrough's declaration reviews each of the "punch list" items before the Commission, explaining for each item law enforcement's traditional capabilities in the POTS (Plain

Old Telephone Service) environment, the effect of intervening technological changes on those capabilities, and the consequences of omitting the punch list item from the J-Standard.

Finally, we present a declaration by John W. Cutright, an FBI electronics engineer. Mr. Cutright's declaration addresses various technical issues that have been identified in other parties' comments. His declaration provides background information regarding the structure of the Public Switched Telephone Network (PSTN) and the technological changes that the PSTN is currently undergoing. Against that background, he discusses each of the "punch list" items from a technical perspective and addresses technical points raised by the other commenters.

I. General Comments

A. The Basic Policies of CALEA

Many commenters argue that, at the most general level, the Commission's tentative conclusions regarding the deficiencies in the J-Standard are at odds with the basic policies of CALEA. These arguments take several forms. Some commenters argue that CALEA was intended to "preserve the status quo" and that, insofar as the Commission's tentative conclusions would make it possible for law enforcement to carry out surveillance orders that it was previously unable to execute, the Commission is ignoring Congress's supposed status-quo goal. Other commenters argue that Congress intended for CALEA's assistance capability requirements to be construed narrowly, and that the Commission's tentative conclusions are not faithful to that mandate. Still other commenters argue that the Commission is failing to perform its obligations under Section 107(b) by restricting its attention to the provisions of the J-Standard that have been placed in dispute and not reviewing, or otherwise taking account of, the J-Standard's uncontested provisions.

These comments reflect fundamental errors regarding the policies underlying CALEA and the responsibilities of the Commission in giving effect to the statute. We have addressed the basic policies of CALEA at length in our earlier filings, and we encourage the Commission to review those filings for a complete discussion of CALEA's policies. See Government Petition at 11-19; Government June Reply Comments at 3-11. In response to the charges that the Commission has set itself at odds with the policies embodied in CALEA, a few additional remarks are in order.

The argument that the Commission is flouting Congress's "status quo" objective rests on a misunderstanding of the "status quo" that Congress meant to preserve. As we have explained in detail in our earlier filings, the legislative history of CALEA makes clear that Congress wished to leave unchanged law enforcement's legal authority to carry out electronic surveillance. See Government June Reply Comments at 7-10. There is no indication, however, that Congress also meant to leave unchanged law enforcement's technical capability to engage in legally authorized electronic surveillance. To the contrary, CALEA was enacted precisely because technological changes were driving a growing wedge between what law enforcement was legally authorized to do and what it was technically able to do. Far from simply freezing the "status quo" regarding law enforcement's technical capabilities, CALEA represents an unprecedented mandate to close the gap by requiring industry to bring those capabilities into line with the scope of existing legal authorization. See, e.g., House Report at 12, reprinted in 1994 USCCAN at 3492 (CALEA is intended, inter alia, to deal with "impediments to authorized wiretaps, like call forwarding, [that] have long existed in the analog environment").

It should be added that if the relevant standard under CALEA were the preservation of law enforcement's traditional technical surveillance capabilities, that would argue strongly in favor of most

of the assistance capabilities that are at issue in this proceeding. For example, law enforcement traditionally has had the capability to detect "post-cut-through" dialed digits by monitoring the local loop between the subscriber's terminal and his carrier's central office. See Yarbrough Dec. ¶¶ 53-54. As we have explained before, and as we discuss further below, the J-Standard manifestly fails to preserve this capability. If traditional capability is the benchmark, the debate over post-cut-through digits must be resolved in the government's favor. More generally, any commenter who argues that CALEA was meant to guarantee law enforcement exactly the same capabilities that it has historically enjoyed is thus effectively, if unwittingly, conceding that the J-Standard must be modified in a number of important respects.[1]

The argument that the Commission has given an impermissibly "broad" reading to CALEA, rather than a "narrow" reading, is equally misconceived. In each case where the Commission has tentatively concluded that the J-Standard is deficient, the Commission's conclusion is entirely consistent with the language, legislative history, and policies of CALEA. See pp. 21-30, 32-34, 40-43, 44-45, 49-50 infra; see also Government December Comments at 37-38, 44-45, 48-49, 52-53, 54-56, 66-67. All too often, the commenters use "broad" and "narrow" as terms of opprobrium and encomium, rather than engaging in a close consideration of the legal issues. Simply labeling the Commission's reading of CALEA as "broad" does nothing to advance the legal analysis.

Finally, the Commission is acting entirely properly in directing its attention to the portions of the J-Standard that have been called into question by the several rulemaking petitions here, rather

---

[1] As noted above, the Yarbrough declaration contains a full discussion of law enforcement's traditional electronic surveillance capabilities. We refer the Commission to this discussion in connection with the claims by various commenters that one or another "punch list" item exceeds law enforcement's traditional capabilities.

than embarking on an omnibus review of the J-Standard as a whole. Contrary to the suggestion of commenters like EPIC, the Commission is not "foreclosing" challenges to other portions of the J-Standard when it confines itself in this proceeding to the specific provisions of the J-Standard that the petitioning parties have placed in controversy. Any person may invoke the Commission's rulemaking authority under Section 107(b) by filing a petition that identifies deficiencies in an industry "safe harbor" standard. See 47 U.S.C. § 1006(b) (petition may be filed by "a Government agency or any other person"); House Report at 18, reprinted in 1994 USCCAN at 3498 (CALEA "[a]llows any person, including public interest groups, to petition the FCC for review of standards implementing wiretap capability requirements"). If EPIC or anyone else believes that the J-Standard has deficiencies other than those that have been identified thus far, they are perfectly free to seek redress by filing their own petitions under Section 107(b). They have not done so. In the absence of additional petitions, nothing requires the Commission to search for controversies where none yet exist.

B. Cost Considerations

The Commission's Notice raises a variety of questions relating to the role of cost considerations in this proceeding. In our comments, we responded to these questions at length. See Government December Comments at 8-18. In response to the Commission's inquiries, the industry commenters offer a welter of cost-related assertions. Unfortunately, these assertions suffer from both legal and factual shortcomings.

1. As we have pointed out in our earlier comments, any consideration of the costs associated with CALEA's assistance capability requirements must take careful account of the statutory context of this proceeding. See Government December Comments at 8-15. Section 107(b) of CALEA is

designed to bring carriers into compliance with CALEA's assistance capability requirements, by eliminating deficiencies in industry standards that would otherwise constitute a "safe harbor" under Section 107(a). The Commission's task under Section 107(b) is two-fold: first, it must determine whether the J-Standard is deficient, and second, it must develop modified standards that correct any identified deficiencies.

Cost considerations have no role to play in the first of these two tasks. For reasons explained in our earlier comments, the scope of CALEA's assistance capability requirements does not turn on the costs of implementing those requirements. See Government December Comments at 9-15. Congress recognized that meeting CALEA's assistance capability requirements might be prohibitively expensive for individual carriers, but its response was not to pare these requirements down to accommodate carriers for which compliance would be particularly expensive, but rather to permit individual carriers to seek relief under Section 109(b). As a result, the Commission can and should determine whether the J-Standard is deficient, in the first instance, without determining the costs entailed in correcting the deficiencies.

Cost considerations do have a role to play in the second stage of the Commission's deliberations under Section 107(b), but only a limited role. Once it has identified deficiencies in the J-Standard, the Commission must correct these deficiencies by developing new standards that: (i) meet the assistance capability requirements of Section 103 by cost-effective methods; (ii) protect the privacy and security of communications not authorized to be intercepted; (iii) minimize the cost of compliance on residential ratepayers; (iv) serve the policy of encouraging the provision of new technologies and services to the public; and (v) provide a reasonable time and conditions for compliance with and the transition to any new standard. 47 U.S.C. § 1006(b). These provisions

make cost considerations relevant in determining how identified deficiencies in the J-Standard are to be corrected. They do not, however, make cost a basis for determining whether deficiencies are to be corrected. See Government December Comments at 11-13. Congress has already resolved the question of whether the Commission must correct identified deficiencies, by mandating that the Commission's technical standards "meet the assistance capability requirements of section 1002 of this title [Section 103 of CALEA]." Id. § 1006(b)(1).

Within this statutory framework, comparative cost information -- i.e., information about the relative costs of alternative methods of correcting deficiencies in the J-Standard -- may well be relevant to the Commission's task. For example, if the Commission found itself presented with two alternative means of correcting a particular deficiency, one of which was appreciably less expensive than the other but equally effective, the Commission might well choose the less expensive alternative as the more "cost-effective method" (47 U.S.C. § 1006(b)(1)) of meeting CALEA's assistance capability requirements. By the same token, choosing the least expensive method of curing a deficiency may tend to "minimize the cost of * * * compliance on residential ratepayers" (id. § 1006(b)(3)). But in the absence of comparative cost information, assertions that a particular capability is "costly" or "expensive" are not legally germane under Section 107(b).

The cost estimates offered by the industry commenters simply fail to take account of this legal framework. Even if the industry cost estimates could be considered reliable (and, as we discuss below, they cannot), they suffer from three legal flaws, each of which makes them unsuitable as a basis for the Commission's deliberations.

First, most of the industry cost estimates are not directed at the incremental cost of implementing the additional assistance capabilities that are the subject of this proceeding. Instead,

many industry commenters discuss the cost of implementing the J-Standard, either on their own networks (GTE Comments at 7; BellSouth Comments at 2; AT&T Comments at 28; Nextel Comments at 22) or across the entire industry (CTIA Comments at 2; SBC Comments at 5). The Commission has already made plain that the unchallenged portion of the J-Standard is not at issue in this proceeding (see Notice ¶ 45), and properly so. The costs that carriers will incur in implementing undisputed assistance capability requirements are no more germane to this proceeding than any other costs that carriers are legally obligated to bear, such as the costs of complying with federal securities laws or occupational safety and health laws. Nothing in Section 107(b) authorizes the Commission to excuse carriers from the costs of satisfying undisputed statutory mandates on the ground that compliance would be "too expensive." When commenters complain about "the CALEA surcharge" (CTIA Comments at 18), or argue that CALEA compliance will be particularly expensive for wireless carriers (Bell Atlantic Mobile Comments at 9), their complaints should be directed to Congress, not to the Commission. Thus, the costs of complying with the undisputed assistance capability obligations incorporated in the J-Standard cannot legitimately justify the failure to correct identified deficiencies in the J-Standard, and estimates of those costs have no proper role to play in this proceeding.

Second, the industry cost estimates that are directed at the cost of the punch list items tend to address those costs in the aggregate, rather than attempting to identify the costs associated with individual capabilities. Several commenters proffer estimates of carrier-specific or industry-wide costs of implementing the entire punch list (SBC Comments at 5; AirTouch Comments at 13), or the

J-Standard plus the entire punch list (USTA Comments at 8).[2] But the Commission's task is not to make an "all or nothing" choice between adding the punch list in toto or leaving the J-Standard unchanged. Instead, the Commission must decide whether each individual capability identified in the government's rulemaking petition should be added to the J-Standard.[3] Estimates of the aggregate cost of implementing all of the punch list capabilities are irrelevant to the Commission's task in determining whether to add individual capabilities to the J-Standard.

Finally, in the few instances where commenters have attempted to provide cost estimates for individual punch list items, they have made no attempt to identify any less expensive alternatives for correcting the deficiency at which the item is directed. For example, the commenters that refer to the hardware costs that could be incurred in connection with detecting post-cut-through dialing (USCC Comments at 10; SBC Comments at 6; AirTouch Comments at 13) make no effort to show that the underlying deficiency in the J-Standard could be corrected in a more "cost-effective" manner than we have suggested. Tellingly, one commenter concedes that, unless the Commission radically alters its tentative conclusions and decides that the J-Standard has no deficiencies at all, the addition or removal of particular punch list items will not substantially affect the carriers' compliance-related costs. See BellSouth Comments at 6 ("the Commission's selective pruning of punch list items will not substantially reduce carriers' capital and expense costs").

---

[2] It is not entirely clear whether USTA's estimate addresses the costs associated with the J-Standard, or the J-Standard plus the punch list.

[3] At least one carrier appears to understand this point, when it notes that the kind of cost information that could be useful to the Commission would be a "breakdown of the costs of individual punch list items or other capabilities." US West Comments at 4.

In sum, as a legal matter, the industry cost comments are far more significant for what they do not say than for what they do say. If the carriers had information demonstrating that an alternative method of curing a particular deficiency would be more "cost-efficient" than the corresponding method suggested by law enforcement, the carriers presumably would have provided the Commission with this information. They have not.

It makes no sense for telecommunications carriers to suggest in their comments that the government bears the burden of demonstrating that its proposed means of correcting the J-Standard's deficiencies are more "cost-effective" than any conceivable alternative means of curing those deficiencies. See, e.g., US West Comments at 4. The carriers themselves are obviously the parties most familiar with the deployment costs associated with meeting CALEA's assistance capability requirements, for it is the carriers that deploy new features on the nation's telecommunications networks.[4] Yet, with minor exceptions, these commenters have failed to identify any alternative methods of correcting the J-Standard's deficiencies. In the absence of a showing that workable alternatives exist, there is simply nothing with which to compare the costs of the punch list items, and no basis for arguing that the punch list items are not "cost-effective methods" of satisfying the requirements of Section 103.

---

[4] The manufacturers are the parties most familiar with the costs of developing, as distinct from deploying, CALEA solutions. We understand that several manufacturers have submitted cost information to the Commission, accompanied by requests for confidential treatment under 47 C.F.R. § 0.459. The Commission's general policy is not to accord confidential treatment to materials submitted in rulemaking proceedings. See Report and Order, In the Matter of Examination of Current Policy Concerning the Treatment of Confidential Information Submitted to the Commission, GC Docket No. 96-55, ¶¶ 43-44 (released Aug. 4, 1998). If the Commission decides to depart from that general policy in this case, it should permit interested parties to examine the manufacturer submissions pursuant to an appropriate protective order. See id. ¶ 45.

2. For the foregoing reasons, even if the cost estimates submitted by the industry commenters were factually accurate, they would not provide the Commission with any legal basis for failing to correct deficiencies in the J-Standard. Having said that, we add that the commenters' cost estimates appear to be grossly overstated. A brief explanation of the process for achieving CALEA compliance will help to explain why.

The features required for a carrier to meet its CALEA assistance capability obligations will be among many features contained in one or more periodic "releases" deployed on the carrier's switches. These releases, which consist primarily of software but may include hardware elements as well, are purchased by carriers from switch manufacturers and are analogous to software releases used in personal computing, like the "Windows 98" release of Microsoft's operating system replacing the "Windows 95" release. Like ordinary business software releases, telecommunications switch releases are an entrenched element of the business cycle, rather than an unusual event -- i.e., most carriers will purchase periodic releases from the switch manufacturers regardless of what happens in this proceeding, and would have done so even if CALEA had never been enacted. The only impact that this proceeding may have on that process is that it may cause particular releases to include one or more features designed to cure deficiencies in the J-Standard. The costs attributable to CALEA are only those that will be added to the costs of the regular release process by the addition of the CALEA features.

The essential process of deploying a release is the same, regardless of the particular features included in it. As a result, the addition of "punch list" features is not likely to cause significant cost increments in the process of deploying switch releases. This is consistent with BellSouth's

acknowledgment, noted above, that the addition of individual punch list items will not give rise to "substantial" marginal costs for the carriers. BellSouth Comments at 6.

Several commenters do proffer estimates of the overall costs, including the costs of purchasing the necessary releases and deploying them on a particular network or across portions of the industry, of the J-Standard. For example, GTE claims that the cost of implementing the J-Standard for its wireline and wireless companies will exceed $400 million, and that sundry other improvements could add another $300 to $400 million. GTE Comments at 7. BellSouth estimates its cost of complying with the J-Standard at $388 million or more. BellSouth Comments at 2. AT&T Wireless Services, Inc. estimates its cost of complying with the J-Standard at over $35 million. AT&T Comments at 28. USTA estimates the aggregate compliance cost for its member companies (either for the J-Standard or for the J-Standard plus the punch list) at $2.2 to $3.1 billion. USTA Comments at 8. CTIA offers the most lurid estimate, claiming that the industry-wide cost of implementing the J-Standard could be as much as $5 billion. CTIA Comments at 2 ("the hardware and software costs of implementing the industry's standard alone is as much as ten times what Congress authorized the Attorney General to spend [i.e., $500 million] when it passed CALEA in 1994").

Even if the Commission were to determine that these estimates were relevant to its statutory mandate, the Commission would be well advised to approach them with a healthy measure of skepticism. Although the commenters' general lack of explanation and detail make it impossible for us to identify all of the questionable assumptions underlying their numbers, we can discern from the little that they do say, and from the sheer magnitude of their cost assertions, that their estimates appear to reflect several crucial errors and inappropriate assumptions:

* The carriers may be basing their cost assertions on extremely unrealistic estimates of the price they will pay manufacturers for CALEA solutions. None of the carriers claims to have actually completed price negotiations with the manufacturers of their switches, and their comments suggest that, for the most part, these negotiations have not yet even begun. See USCC Comments at 7; AT&T Comments at 26; GTE Comments at 8; CTIA Comments at 8; Nextel Comments at 23. Because the market has not yet set the actual prices of the CALEA features, the carriers are free essentially to pluck their price estimates from the air, or to proffer the prices "quoted" to them by the manufacturers (BellSouth Comments 6) as though they were the actual price to be paid for these features. In reality, of course, the quoted prices are merely the beginning of a negotiation process, and it is general industry practice for carriers to be given substantial discounts, of as much as 65% or more, from those prices.

* Carriers may be attributing to CALEA the entire deployment cost associated with incorporating the release or releases that will include the CALEA features into their networks. Cf. Bell Atlantic Comments at 14; BellSouth Comments at 4. As we have explained above, carriers generally would be deploying these releases even if CALEA had never been enacted, and thus the relevant cost is only the added deployment cost associated with the presence of the CALEA features in one or more releases.

* The carriers may be including in their estimates all of the costs associated with CALEA's capacity requirements. Cf. SBC Comments at 6; USTA Comments at 8; GTE Comments at

7. Most of these costs are to be reimbursed by the government (see 47 U.S.C. § 1003(e)), and therefore do not represent "costs" to the industry. Moreover, the carriers may be vastly overstating these costs by estimating the cost of providing the county-wide aggregate capacity requirements on every switch within each county. Cf. USTA Comments at 8. These county-wide aggregate requirements, however, are just that: they represent the aggregate capacity that a carrier must make available within the specified county, not the capacity that must be provided on every switch within the county. See 63 Fed. Reg. 12,218, 12,235 (1998).

* The carriers may base their estimates on the premise that compliance solutions must be incorporated into every switch in their networks. For many platforms, however, compliance solutions need only be incorporated into the subset of "host" and "stand-alone" switches, not into "remote" switches. For these platforms, remote switches essentially share the brains of host and stand-alone switches, and thus if the CALEA features are available at a host or stand-alone switch, they are also available at any interlinked remote switches.

* Carriers may be singling out the types of switch that will be most expensive and difficult to bring into compliance with CALEA, leading to an incorrect inference that the costs associated with such switches are representative of the broader costs of compliance in the industry. See AirTouch Comments at 13 ("In one case, the punch list software releases would cost nearly twice as much as the J-STD-025 software release") (emphasis added).

* Carriers may be describing the special hurdles to compliance that would be faced by small, rural telephone companies using unsophisticated switches, overlooking the fact that such a

carrier's switches are very likely to have been installed or deployed before January 1, 1995, and thus to be "grandfathered" pursuant to Section 109 such that the government would reimburse any compliance costs (unless they are "replaced or significantly upgraded or otherwise undergo[] major modification)." 47 U.S.C. § 1008(d); cf. USTA Comments at 8.

* Carriers may be attempting to ascribe to CALEA a variety of costs that they would sustain even in the absence of CALEA, including ongoing network management costs and the costs of conducting wiretaps. Cf. Nextel Comments at 24; AT&T Comments at 29; GTE Comments at 7 n.13.

* Carriers may be counting costs associated with features that law enforcement is not seeking in this proceeding. See SBC Comments at 6 (singling out the cost of "separated delivery," a feature that the government's rulemaking petition does not seek).

3. In addition to proffering generalized assertions about the costliness of CALEA compliance, a few commenters warn that meeting CALEA's assistance capability obligations could dramatically affect consumer demand for telecommunications services. CTIA asserts that the price elasticity of demand for wireless service is -0.51, and argues that this means that "for each dollar increase in the price for services, there will be a corresponding, negative impact of more than 50% in demand." CTIA Comments at 15. This claim is off by almost two orders of magnitude. The price elasticity of demand coefficient represents the percentage by which demand will fall in connection with a one percent increase in price. See Paul A. Samuelson & William D. Nordhaus, Economics 65 (14th ed.

1992). Thus, if the price elasticity of demand were -0.51, a one percent increase in the price would bring about a decline in demand of just over one-half of one percent.

At any rate, there is no basis for the assertion that requiring any or all of the punch list items would have a discernible impact upon telecommunications markets, particularly if no individual punch list item would "substantially" affect the carriers' capital and expense costs (BellSouth Comments at 6). The carriers do not reveal the methodology by which they determine that ratepayers will face any — much less "enormous" (GTE Comments at 9) — new burdens as a result of the addition of the punch list items to the J-Standard. See AT&T Comments at 29; CTIA Comments at 13. But it is difficult to see what conceivable methodology would support such an assertion. Currently, there are approximately 163 million switched access lines and approximately 70 million cellular and PCS subscribers in the United States. Even accepting CTIA's worst-case scenario of $5 billion in industry-wide compliance costs to implement the J-Standard, if the industry spreads these costs over only a five-year period, the resulting increase in the average ratepayer's monthly bill would amount to just under 36 cents. And that assumes that the industry will pass along every dollar of additional costs to consumers, rather than absorbing a portion of the costs out of the industry's many billions of dollars of annual profits.

In summary, we reiterate that information regarding the costs of CALEA compliance is relevant to this proceeding only insofar as it can assist the Commission in selecting the methods of curing any deficiencies in the J-Standard that are "cost-effective," and that "minimize" the burden of compliance on residential ratepayers. 47 U.S.C. § 1006(b)(1), (3). Very little of the cost-related information that the industry commenters have submitted is relevant to this statutory mandate, and although we have attempted to alert the Commission to likely factual errors in the carriers' estimates,

we urge the Commission simply to set aside any cost-related assertions not directly relevant to its statutory responsibilities.

4. In our earlier comments, we noted that manufacturers have provided the government with CALEA price information (as distinct from cost information) pursuant to non-disclosure agreements. Government December Comments at 16. Some commenters argue that this information is relevant to this proceeding and the government therefore should disclose it to the Commission and the other commenters. See U S West Comments at 5; CTIA Comments at 7.

The price information that we have received from manufacturers is not broken down by individual "punch list" items, nor does it identify the relative costs of alternative means of curing the deficiencies identified in the J-Standard. Thus, for the reasons explained above, it is not relevant to the factors enumerated in Section 107(b). In any event, we cannot release this information to the Commission or to the other parties in this proceeding because the non-disclosure agreements preclude us from doing so. Although the commenters invite us to release the information in aggregated form, we have reviewed the non-disclosure agreements and have determined that the release of the information even in aggregated form could reasonably be claimed to violate the agreements. The same limitations preclude us from providing, as several commenters demand, the confidential manufacturer information underlying the CALEA implementation report that was presented by the Attorney General to Congress last year. See Government June Reply Comments at 36 n.21.

C. The Obligation to Deliver Call-Identifying Information

Section 103(a)(2) of CALEA obligates a carrier to ensure that its equipment, facilities, and services are capable of "expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier * * * ." 47 U.S.C. § 1002(a)(2). Many of the comments take issue with the Notice regarding the scope of this statutory obligation. In some instances, commenters argue that information that the Commission has tentatively held to be required by Section 103(a)(2) does not constitute "call-identifying information." In other instances, commenters argue that the information is not "reasonably available," and therefore is outside the scope of Section 103(a)(2) even if it does constitute call-identifying information.

To the extent that these arguments are confined to specific assistance capability items, we address them in Part II below, in connection with our discussion of those items. To a considerable extent, however, the commenters' arguments raise more general issues regarding the meaning and scope of CALEA's provisions regarding call-identifying information. We address those general issues here.

1. CALEA contains an explicit and comprehensive definition of "call-identifying information": "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). We set out this statutory definition at the outset because many of the commenters simply disregard it. They present arguments about the meaning of "call-identifying information" that make no reference to, and are inconsistent with, the

actual terms of the definition that Congress incorporated into CALEA. It is therefore vital to look to the actual statutory definition as the Commission sorts through the commenters' arguments.

Rather than address the definition of "call-identifying information" prescribed by CALEA, many of the commenters turn to a passage in the House Report that discusses the subject of call-identifying information. See, e.g., CTIA Comments at 21 (quoting House Report at 21, reprinted in 1994 USCCAN at 3501); PCIA Comments at 8 (same). As a general matter, when a statutory term is expressly defined in the statute itself, the Commission should not disregard the explicit terms of the statutory definition in favor of language in a committee report. In this case, that general principle takes on added force in light of one critical fact: the quoted passage in the House Report reflects an earlier version of the legislation, one that employed a different definition from the one ultimately adopted by Congress. As a result, it is an unreliable guide to the meaning of the definition that is actually embodied in CALEA.

As we have explained in previous filings, the bill that evolved into CALEA originally referred to "call setup information," which was defined as "the information generated which identifies the origin and destination of a wire or electronic communication placed to, or received by, the facility or service that is the subject of the court order or lawful authorization * * * ." Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearings before the Subcomm. on Technology and the Law, Senate Comm. on the Judiciary, and Subcomm. on Civil and Constitutional Rights, House Comm. on the Judiciary, 103d Cong., 2d Sess. 267-68 (Aug. 11, 1994). Relatively late in the legislative process, Congress replaced "call setup information" with "call-identifying information." In so doing, it adopted a revised definition that both clarified and expanded the scope of the information covered by the term. See Government June

Reply Comments at 31-32. For example, the definition of "call setup information" covered only the "origin" and "destination" of communications; the definition of "call-identifying information" covers not only "origin" and "destination," but also "direction" and "termination." 47 U.S.C. § 1001(2).

It is this revised and expanded definition that Congress adopted when it enacted CALEA. The cited passage in the House Report, however, recites verbatim the superseded definition of "call setup information": "information generated that identifies the origin and destination o[f] a wire or electronic communication placed to, or received by, the facility or service that is the subject of the court order or lawful authorization." House Report at 21, reprinted in 1994 USCCAN at 3501. Whether from oversight or inertia, the committee staff who drafted the report simply failed to reflect the changes to the statutory definition that Congress ultimately approved. Because the report is written in terms of a definition that had been superseded by the time CALEA became law, the language in the report cannot be treated mechanically as a proxy for the definition actually adopted and written into law by Congress.

2. Many commenters argue that various kinds of information are outside the scope of Section 103(a)(2) because they do not constitute call-identifying information "from the perspective of," or "for," or "as to," particular carriers. This line of argument is central, for example, to the commenters' discussion of post-cut-through dialed digits. The commenters argue that because originating carriers do not use post-cut-through DTMF (Dual-Tone Multi-Frequency) tones 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. See, e.g., TIA Comments at 40.

The same kind of argument underlies CDT's position regarding packet mode communications. See CDT Comments at 13-31. CDT asserts that call-identifying information is a "subjective" or "relative concept" that depends on "the perspective of the particular telecommunications carrier upon which an interception order is served." Id. at 23, 25, 29. According to CDT, information in a packet header constitutes "call-identifying information" only if it is information that the carrier carrying out the surveillance order uses to route the packet through its network. Even if the information is used for routing purposes by another carrier, the information does not (in CDT's view) constitute call-identifying information "for" the carrier that is performing the surveillance. Thus, CDT argues that a carrier is obligated under Section 103(a)(2) to provide law enforcement only with "the transactional information [in packet headers] that it uses to process communications," not "the transactional information used by other carriers." Id. at 13 (emphasis in original).

The central problem with these arguments is that they ignore 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 the delivery of 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 "subjective" or "relative," as CDT would have it. 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, for example, 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 simply is no room in the statutory definition to exclude such information based on the use to which it is put by a particular carrier.[5]

The language of Section 103(a)(2) is equally inhospitable to the commenters. 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.[6]

---

[5] It is worth noting that 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.

[6] For reasons that we have discussed previously, Section 103(a)(2)'s "reasonably available" proviso does not excuse carriers from providing call-identifying information that is used by other carriers for call routing purposes. See Government December Comments at 23-24.

CDT and other commenters quote a statement in the House Report that "[f]or voice communications," call-identifying information is "typically" information that "identif[ies] the numbers dialed or otherwise transmitted for the purpose of routing calls through the telecommunications carrier's network." House Report at 21, reprinted in 1994 USCCAN at 3501. The commenters reason that this statement excludes information that is transmitted for the purpose of routing telephone calls through other carriers' networks. But the quoted language does not purport to be exhaustive; by its terms, it merely describes the "typical" case, not all cases. It therefore is entirely consistent with the application of Section 103(a)(2) to call-identifying information (such as post-cut-through dialed digits) that is transmitted through one carrier's network in order to be used for call routing by another carrier.

3. Section 103(a)(2) obligates a carrier to provide law enforcement with access to all call-identifying information that is "reasonably available to the carrier." 47 U.S.C. § 1002(a)(2). Predictably, the industry commenters argue that much of the call-identifying information at issue in this proceeding is not reasonably available. A few of the more ambitious commenters, such as TIA, go so far as to claim that none of the information is reasonably available. See, e.g., TIA Comments at 24 ("All of the call-identifying information sought by the FBI in this proceeding is not reasonably available").

Many of these comments are predicated on the J-Standard's definition of "reasonably available," which provides that call-identifying information is deemed to be "reasonably available" only if it is "[1] present at an Intercept Access Point (IAP) [2] for call processing purposes." J-STD-025, § 4.2.1 (brackets added). In our comments, we reviewed this industry definition in considerable detail and identified several major shortcomings in it. See Government December Comments at 20-

25. To the extent that the current round of industry comments rests on the J-Standard definition, we refer the Commission to our prior discussion.

In addition to invoking the J-Standard definition of "reasonably available," some industry commenters argue that the call-identifying information at issue here is not available at all in existing networks, and hence cannot be deemed "reasonably available." In reviewing this argument, it is vital for the Commission to understand one central point: all of the call-identifying information to which the government is seeking access in this proceeding is already present in one form or another within existing networks. For example, information about which parties are connected to a multi-party call over the course of the call is present within (and used by) the network elements that are handling the call. If it were otherwise, the network could not maintain the required connections and could not add and release network resources at the proper times. Similarly, when a subject presses feature keys or engages in other dialing and signaling activity during the course of a call, the carrier's switch receives the resulting signals that are generated by the subject's terminal equipment. The same thing is true with respect to post-cut-through dialing. And network-generated in-band and out-of-band signaling is, by definition, generated by (and hence present in) the network itself. Thus, carriers are not being called on to "create" call-identifying information that does not already exist.

The commenters try to obscure this point by arguing that the messages that are to be used in delivering the requested call-identifying information to law enforcement do not now exist. See, e.g., CTIA Comments at 25-26; Nextel Comments at 9. It is perfectly true that the specific messages discussed in the government's rulemaking petition, such as the proposed PartyJoin and PartyDrop messages (Government Petition, Appendix A, p.5), are not currently in use. But that is equally true of the messages contained in the J-Standard itself. Under the J-Standard, "call-identifying information

is formatted into discrete messages using a specialized protocol" called the Lawfully Authorized Electronic Surveillance Protocol (LAESP). See J-STD-025, § 4.2.3. The LAESP and its constituent messages are defined by the J-Standard itself. See id. §§ 6.2.1-6.2.3, 6.3.1-6.3.10, 6.4.1-6.4.11. No carrier network currently generates these messages, and in the absence of CALEA, no network would do so. Instead, a carrier that wishes to avail itself of the J-Standard's safe harbor must modify its network to generate them. As the J-Standard itself recognizes, what matters for purposes of a carrier's obligations under Section 103(a)(2) is the reasonable availability of the underlying call-identifying information, not the presence or absence of pre-existing messages encapsulating that information in a particular form. The messages are "envelopes" for delivering call-identifying information; they are not the call-identifying information itself.

In a variation on the foregoing argument, several commenters argue that Section 103(a)(2)'s "reasonably available" language excuses a carrier from providing law enforcement with access to any call-identifying information if the carrier would have to modify its network equipment to do so. See, e.g., TIA Comments at 23-24; USTA Comments at 3. This argument is a breathtaking one, for it flies in the face of one of CALEA's fundamental principles: "telecommunications carriers * * * are required to design and build their switching and transmission systems to comply with the legislated requirements." House Report at 18, reprinted in 1994 USCCAN at 3498 (emphasis added). CALEA was enacted precisely because Congress was not willing to consign law enforcement to whatever information a carrier might otherwise design its network to provide. If TIA were correct that carriers are under no obligation to modify their equipment to provide law enforcement with access to call-identifying information, there would have been no need for Section 103(a)(2) at all.

In an effort to support this argument, the commenters point to a passage in the legislative history that states that if call-identifying information "is not reasonably available, the carrier does not have to modify its system to make it available." House Report at 22, reprinted in 1994 USCCAN at 2502. But the quoted language offers no assistance to the commenters, for by its terms, it presupposes that the information in question "is not reasonably available" (emphasis added). If particular call-identifying information is reasonably available, nothing in this language excuses a carrier from its express statutory obligation to "ensure that its equipment, facilities, or services * * * are capable of * * * expeditiously isolating" the information and "enabling the government * * * to access" it. 47 U.S.C. § 1002(a)(2).

Finally, AT&T states that call-identifying information is not reasonably available to a carrier if it is associated with processing that takes place entirely within the subscriber's terminal or other equipment owned and maintained by the subscriber, and the carrier therefore "is not aware of it." AT&T Comments at 6; see also TIA Comments at 22 (call-identifying information is not "reasonably available" if it resides "in a portion of the network not accessible to a carrier," such as a PBX). We agree. We have never suggested, as TIA claims, that "reasonably available" means "available anywhere in any network." TIA Comments at 22 (emphasis added). Rather, the information must be present in the carrier's own network. See Government December Comments at 25. We are not asking carriers to create information that cannot be found in their networks.

D. The Section 107(b) Criteria

As discussed above and in our earlier comments, Section 107(b) sets forth several criteria to be taken into account by the Commission in modifying deficient industry "safe harbor" standards. 47 U.S.C. § 1006(b)(1)-(5); see Government Petition at 59-63; Government December Comments at

27-28. Some of the commenters argue that these criteria form an additional hurdle (or series of hurdles) that law enforcement must surmount before it is entitled to have the Commission cure the deficiencies in the J-Standard. See, e.g., Nextel Comments at 21; PCIA Comments at 7-8; US West Comments at 2. Under this view, even if the Commission determines that the J-Standard is missing a capability required by Section 103, the Commission must leave that deficiency in place unless the Commission determines that eliminating the deficiency would "meet" the criteria of Section 107(b).

This argument radically misstates the purpose of Section 107(b) and the Commission's responsibilities under that provision. The fundamental purpose of Section 107(b) is to ensure that carriers meet the assistance capability requirements of Section 103, not to excuse carriers from meeting those requirements. If the Commission determines that the J-Standard is deficient in one or more respects, as it has already tentatively concluded, then the Commission must modify the J-Standard to eliminate those deficiencies. The language of Section 107(b) could hardly be any clearer on this point: if an industry standard is deficient, Section 107(b) directs the Commission to establish technical requirements or standards that "meet the assistance capability requirements of section 1002 of this title" (that is, Section 103 of CALEA). 47 U.S.C. § 1006(b)(1) (emphasis added). A Commission order in this proceeding whose provisions did not require carriers to "meet the assistance capability requirements" of Section 103 would be in patent conflict with Section 107(b) itself.

As we explained in our earlier comments, the criteria of Section 107(b) are directed at how the Commission should cure identified deficiencies in industry safe-harbor standards, not at whether the Commission should cure such deficiencies. See Government December Comments at 11-12, 27-28. If the Commission identifies more than one workable means of eliminating a particular

deficiency, then the criteria in Section 107(b) may and should inform the Commission's choice among the available alternatives. But the criteria provide no basis whatsoever for allowing a deficiency to remain uncorrected. To treat the statutory criteria as additional preconditions for relief would be to transform Section 107(b) from what Congress intended -- a means of correcting deficient industry standards -- into its diametrical opposite.

II. Comments Regarding Particular Assistance Capabilities

A. Conference Call Content

1. The Commission has tentatively concluded that Section 103(a)(1) of CALEA requires carriers to provide law enforcement with access to all content of subject-initiated conference calls supported by the subscriber's equipment, facilities, and services, including communications between parties on other legs of a conference call when the subject places those other legs on hold or drops off the call. Notice ¶¶ 77-78. In our comments, we agreed with this tentative conclusion and addressed various questions raised by the Notice in connection with this capability. See Government December Comments at 37-44.

Many commenters argue that when a subject places the other legs of a conference call on hold or hangs up, communications among the other participants fall outside the scope of the carrier's assistance capability obligations under Section 103(a)(1). We have addressed this argument at length in our earlier filings, and we refer the Commission to our prior comments. By its terms, Section 103(a)(1) obligates a carrier to provide law enforcement with "all wire and electronic communications * * * to or from equipment, facilities, or services of a subscriber of such carrier." 47 U.S.C. § 1002(a)(1) (emphasis added). As we have explained previously, when a subscriber's service supports the ability of other participants in a conference call to continue to speak to one another when

the subscriber places them on hold or hangs up, their conversations constitute "communications * * * to or from" the subscriber's "equipment, facilities, or services," and therefore come squarely within the scope of Section 103(a)(1). See Government June Reply Comments at 17-21; Government December Comments at 38-39.

PCIA argues that when parties on held legs of a conference call speak to each other, their communications are carried "through," rather than "to or from," the subscriber's equipment, facilities, and services. See PCIA Comments at 23. PCIA's reasoning appears to be that a communication is not carried "to or from" a subscriber's equipment, facilities, or services unless it is routed by the subscriber's switch to his terminal equipment. But if that were the case, then call forwarding would be outside the scope of CALEA: when call forwarding is activated, incoming calls are not routed to the subscriber's terminal, but instead are routed to another destination (in some cases, a destination served by an entirely different carrier). Yet the legislative history makes abundantly clear that call forwarding was one of the principal features that Congress intended to reach when it enacted CALEA. See House Report at 9, 20, reprinted in 1994 USCCAN at 3489, 3500. The statutory language readily accommodates this legislative goal, because a forwarded call is carried "to" and "from" the subscriber's equipment, facilities, and services. Precisely the same thing is true of the held legs of conference calls supported by the subscriber's conference calling service.

2. Several commenters assert that so-called "meet me" conference service should be excluded from the scope of the Commission's ruling regarding delivery of conference call content. See Ameritech Comments at 6; AT&T Comments at 7-8; CTIA Comments at 24. In a meet-me conference, conference participants connect to a pre-arranged conference bridge using a directory number assigned to the bridge. Meet-me conference service is ordinarily provided on an "on demand"

basis: a party that wishes to set up a meet-me conference contracts with the carrier in advance to make the conference bridge available for a specified number of participants at a particular time.

The commenters assert that meet-me conference service is outside the scope of a carrier's assistance capability obligations under Section 103. That argument, however, is repudiated by the J-Standard itself. The J-Standard treats meet-me conferences no differently from any other multi-party circuit mode communications for purposes of a carrier's obligations under Section 103. See J-STD-025, § 4.5.1, p. 20 (describing the manner in which "[t]he Circuit IAP * * * shall access a multi-party circuit mode communication (e.g., Three-Way Calling, Conference Calling, or Meet Me Conferences)" (emphasis added)).

The commenters argue that CALEA's assistance capability requirements apply only to the services of "subscribers," and that meet-me conference service is not a "subscriber-based" service because it is provided on demand to any party that makes the necessary arrangements in advance. But a party that contracts for meet-me conference service is no less a "subscriber," for purposes of CALEA, than a party that arranges for conventional conference calling service; the only difference is the duration of the party's "subscription" for the service. In any event, the assistance capability requirements of Section 103 apply to all "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). Assuming for the sake of argument that a party who arranges for a meet-me conference is not a "subscriber," he necessarily qualifies as a "customer," and hence the equipment,

facilities, and services associated with the meet-me conference come within the scope of the carrier's assistance capability obligations, as the J-Standard itself recognizes.[7]

3. Several commenters raise questions regarding the provisioning of conference call intercepts -- specifically, the number of call content channels (CCCs) that will be required to capture the content of "held" conference legs. See Airtouch Comments at 15; AT&T Comments at 7; CTIA Comments at 23; TIA Comments at 27. If a subscriber's service includes the capability for the parties on held legs of the conference call to speak to each other, law enforcement must provision two CCCs: one CCC for delivery of the contents of the held legs and one CCC for the contents of any concurrent communications between the subscriber and other parties.[8] Contrary to AirTouch's apparent assumption, no more than two CCCs will be required, because law enforcement is not seeking "separated delivery" of each leg of the conference call on a different CCC. As a result, AirTouch's concerns about "porting and trunking costs" (AirTouch Comments at 15) are substantially overstated.

AT&T asserts that the obligation to provide law enforcement with the held legs of subject-initiated conference calls should be conditional on adequate provisioning of CCCs by law enforcement. AT&T Comments at 7. We agree that if law enforcement has not arranged for

---

[7] In general, CALEA tends to use "subscriber" as a shorthand term for any person who is making use of the services of a telecommunications carrier. For example, the definition of "call-identifying information" speaks in terms of "communication[s] generated or received by a subscriber." 47 U.S.C. § 1001(2). No one would seriously suggest that the definition should be read to exclude communications by a subscriber's family members or (in the case of a corporate subscriber) the subscriber's employees. Similarly, in pen register cases, Section 103(a)(2) of CALEA excuses carriers from providing "information that may disclose the physical location of the subscriber." 47 U.S.C. § 1002(a)(2). It would be frivolous to suggest that this privacy provision was meant to protect only subscribers and not other persons who may use a subscriber's wireless handset.

[8] For example, if A (the subscriber) places B and C on hold in order to take an incoming call from D, then one CCC is required to capture the conversation between A and D and a second CCC is required to capture the conversation (if any) between B and C.

adequate provisioning of CCCs, a carrier is under no obligation to deliver call content for which a CCC is unavailable. There is no need, however, for the Commission to address this point separately in its order. As a general matter, the J-Standard already provides that a carrier's obligation to provide access to call content is limited by CCC exhaustion. See J-STD-025, § 4.6.3. That limitation will apply to held legs of conference calls just as it applies to all other multi-party call scenarios in which more than one CCC is required.[9]

4. Bell Atlantic Mobile states that "[e]xisting technologies generally do not continue the connection after the subject terminates his or her connection to the call, yet the first punch list item would make that capability a requirement that all carriers must offer." Bell Atlantic Mobile Comments at 6. This comment reflects a basic misunderstanding of our position. As we have said on more than one occasion in this proceeding, if a carrier does not offer a particular service or feature to its subscribers, we are not asking the Commission to require the carrier to offer the service or feature simply so that law enforcement can monitor communications that would make use of it. If the conference calling service that a carrier makes available to its subscribers does not include the capability for other participants to continue to talk when the subscriber has left the call, then the carrier is under no obligation whatsoever to add that capability. Our position is far more limited: if the carrier does offer such a capability, then (and only then) CALEA obligates it to make the resulting communications available to law enforcement pursuant to appropriate legal authorization.

---

[9] In the case of "meet me" conference service, law enforcement will provision a CCC for delivery of the contents of the conference call from the conference bridge to law enforcement's collection point. For Title III purposes, a meet-me conference bridge ordinarily will constitute a separate "facility" from the local switch associated with the subscriber's own directory number, and law enforcement therefore will be responsible for obtaining a new Title III order that covers the conference bridge.

5. Finally, several commenters argue that Title III does not authorize law enforcement to intercept the remaining legs of a conference call when the subject places the legs on hold or hangs up. See, e.g., EPIC Comments at 20-22; PCIA Comments at 23-24; TIA Comments at 26; US West December Comments at 11-12. The short answer to these arguments is that they raise legal issues that are beyond the scope of this proceeding. The Commission has made clear that its task is not to "define the scope of authorizations needed by LEAs to intercept or obtain call content or call-identifying information," but rather to determine "what capabilities each carrier must provide if and when presented with a proper authorization or court order to expeditiously provide LEAs access to call content and call-identifying information." Notice ¶ 33 (emphasis added). As the Commission has recognized, it only needs to decide what assistance capabilities are required by Section 103(a) of CALEA, not what legal authorization must be in hand for law enforcement to avail itself of those capabilities, or in what circumstances the requisite authority may be obtained.

Even if the commenters' Title III arguments were relevant to the assistance capability issues now before the Commission, they would fail to carry the day, for they rest on a series of misunderstandings regarding the scope and operation of Title III. We have discussed these shortcomings at length in our earlier comments. See Government June Reply Comments at 21-30. The commenters' latest remarks require only a brief additional response.

Several commenters argue that law enforcement lacks authority to monitor the "held" legs of a conference call supported by the subscriber's services because, "once the subject of the warrant has dropped off the call, the carrier will be facilitating the warrantless electronic surveillance of the other parties on the conference call." PCIA December Comments at 23-24 (emphasis in original); see also TIA Comments at 26-27; EPIC Comments at 20-21. These commenters assume that Title III orders

restrict law enforcement to the interception of calls in which a specified criminal suspect is participating. As we have explained previously, that assumption is fundamentally wrong. See Government June Reply Comments at 22-26. Title III expressly authorizes law enforcement to monitor all pertinent conversations that can be intercepted through the telecommunications facilities specified in the interception order, regardless of the identity of the subscriber, the subject, or the other speakers.[10] Even if none of the parties to a particular conversation is named in the interception order, law enforcement may conduct a legal interception, subject to Title III's minimization requirements, if the conversation takes place over the facilities that are subject to the order. United States v. Kahn, 415 U.S. 143, 156-157 (1974).[11]

The commenters also argue that the Commission's tentative conclusion would distort the meaning of "facilities" under Title III. See EPIC Comments at 20-21; PCIA Comments at 24; US West Comments at 12. But as the Commission has pointed out, "the plain language of CALEA's

---

[10] Law enforcement routinely, and properly, performs interceptions where the subscriber whose telecommunications facilities are under surveillance is not a criminal suspect but there is nonetheless probable cause to believe that the facilities will be used in connection with criminal activity. See, e.g., United States v. Miller, 116 F.3d 641, 661-662 (2d Cir. 1997) (interception of the defendant's mother's facilities was proper because the mother's "telephone was used to place calls to many telephones where [gang] members lived or conducted illegal business, and * * * several calls were received from state prisons where gang members were incarcerated"); United States v. Elder, 90 F.3d 1110, 1133 (6th Cir. 1996) (sustaining wiretap of defendant's mother's phone because Title III is satisfied by a showing of "probable cause that the telephone at issue is being used in an illegal operation"); United States v. Meling, 47 F.3d 1546, 1552 (9th Cir. 1995) (explaining that when the defendant moved to his parents' home, "their phone * * * became the target of the wiretap").

[11] The commenters also make the assumption that the subject who drops off the conference call or places the remaining legs of the conference call on hold is the person whom law enforcement suspects of criminal activity. That assumption is likewise incorrect. It may well be that the party whom law enforcement is interested in monitoring is on one of the held legs of the conference call, and that the Title III order is directed at the facilities of a third party because law enforcement has established that those facilities are being used "remotely" by the criminal suspect in this fashion.

Section 103 includes the terms 'equipment' and 'services', in addition to 'facilities.'" Notice ¶ 77. In any event, there is no basis in Title III itself for the commenters' efforts to restrict "facilities" to specific elements of a subscriber's equipment, such as "the connection between a subscriber's phone and the subscriber side port of the carrier's switch" (EPIC Comments at 21) or "the subscriber's CPE, loop or port" (US West Comments at 12). Because a Title III interception order may be directed toward any telecommunications facilities that may be used in furtherance of a crime, rather than simply toward a specified individual, "facilities" must be understood to cover the network elements (such as switches, peripheral devices, and signaling devices) that form the communications pathway where the communications that are subject to interception may be found. As long as law enforcement has probable cause to believe that particular telecommunications facilities are being used for criminal purposes, a court may grant it legal authority under Title III to intercept conversations there. See Government June Reply Comments at 27-30.

In the POTS environment, where all of the communications associated with a particular telephone number ordinarily could be detected over the subscriber's local loop, there was no reason for purposes of Title III interception orders (or judicial opinions analyzing such orders) to distinguish the telephone number from the physical equipment connecting the subscriber to the carrier. See Government June Comments at 28-29. In digital networks, by contrast, a subscriber's features and services may result in communications that have no detectable effect upon the subscriber's terminal equipment because the features and services are activated and implemented at the switch. Interception orders for switch-based electronic surveillance therefore may define the "facility" under surveillance functionally, by reference to the services associated with a particular telephone number or account. For example, a subscriber who invokes call forwarding will not receive calls at the

terminal associated with his telephone number, but an interception order directed at the subscriber's "facilities," defined by reference to his phone number or any other description that satisfies the particularity requirement of the Fourth Amendment (as articulated in Title III by the phrase, "nature and location"), would authorize law enforcement to intercept the forwarded call at the switch. And it is equally clear that Section 103(a)(1) of CALEA requires carriers to have the capability to provide law enforcement with the content of such forwarded calls. See House Report at 9, reprinted in 1994 USCCAN at 3489; see also J-STD-025, § 5.4.7 (Redirection message); id. Annex D, § D.11. The commenters' insistence that Title III "facilities" are restricted to a particular subscriber's terminal equipment is therefore incorrect.[12]

B. Party Join/Hold/Drop Information

The J-Standard does not require carriers to notify law enforcement when parties join a multi-party call, drop from the call, or are placed on hold. The Commission has tentatively concluded that the J-Standard is deficient in this regard and must be modified to ensure that carriers provide law enforcement with reasonably available party join, party hold, and party drop information. Notice ¶¶ 85-86. The commenters raise a number of objections to this conclusion.

1. Some of the commenters argue, as they have before, that information about which parties are connected to a multi-party call does not constitute "call-identifying information." For the most part, we have addressed these arguments in our prior filings, and we refer the Commission to our earlier discussion of this issue. As we have explained, CALEA defines "call-identifying information"

---

[12] However, we are not suggesting (as some commenters claim) that a Title III "facility" could encompass "the entire network to which [a] telephone is attached." PCIA Comments at 24. A Title III facility is confined to the network elements that support and are identifiable with the services associated with the subscriber's telephone number.

to encompass information identifying "the origin, direction, destination, or termination of each communication generated or received by a subscriber * * * ." 47 U.S.C. § 1001(2) (emphasis added). A multi-party call can involve more than one "communication," as different parties join and leave the call; information about which parties are connected to the call identifies the "origin," direction," and "destination" of "each communication" within the call. See Government June Reply Comments at 52-53.

The commenters err by treating a multi-party, multi-leg call as a single "communication." A simple example suffices to show the shortcomings with this approach: assume that the subject is connected to two other people, A and B. The subject places A on hold and discusses a criminal matter with B. The subject then places B on hold and discusses an innocent matter with A. The commenters are asking the Commission to treat the subject's criminal conversation with B and his entirely unrelated, innocent conversation with A as a single "communication." See, e.g., AT&T Comments at 9. Doing so would mean that law enforcement in many instances would lack proof of which party took part in the criminal conversation and which party did not. It would be manifestly contrary to the purposes of CALEA to construe the definition of "call-identifying information" in this fashion.

CTIA and Nextel argue that information about party joins, party holds, and party drops does not constitute "call-identifying information" because party join, hold, and drop messages "do not exist today." CTIA Comments at 25-26; Nextel Comments at 9; see also AT&T Comments at 9 (carriers do not "dynamically report any party's addition to or drop from a conference call") (emphasis added). This argument confuses the information available to the network and the messages used to encapsulate the information and convey it to law enforcement. As explained above, whether

particular information exists in a network is relevant to a carrier's obligations under Section 103(a)(2); whether particular messages are already in existence to deliver that information to law enforcement is not. See pp. 27-28 supra.

US West asserts that party join information identifies the "origination" of a communication, not its "origin." US West Comments at 16. US West's distinction between "origination" and "origin" is, to be charitable, an elusive one. Far from being obviously distinct, the two words are often used interchangeably. See, e.g., Oxford English Dictionary, Compact Edition 2010 (1971) (definition of "origination" includes "origin"); Roget's International Thesaurus §§ 68.1, 153.5 (4th ed. 1977) (listing "origin" and "origination" as synonyms). Thus, saying that party join information identifies the "origination" of the communication is tantamount to conceding that it identifies the communication's "origin."

US West also argues that party drop information does not identify the "termination" of a communication because "termination" refers to the connection that completes a circuit for a communication, not "the end of a call." US West Comments at 15-16. There is no indication that Congress meant to give "termination" the restrictive meaning assigned to it by US West.[13] In any event, even if it were assumed that a party drop does not change the "termination" of a communication, party drop information nevertheless identifies the "direction" and "destination" of the communication that takes place after the dropped party leaves the call. When a subject who has been speaking to two other parties, A and B, continues to speak to A on the remaining call leg after B has

---

[13] US West quotes a passage from the House Report that refers to the "originating and destination numbers of targeted communications." See US West Comments at 15-16 & n.44. This language makes no reference to "termination," and therefore offers no support for US West's reading of that term.

dropped off the call, the direction and destination of the communication is different from what it was when the subject's words were being transmitted across two separate call legs to A and B.

Finally, US West and other commenters argue that the "origin, direction, destination, or termination" of a communication does not change when a party is placed on hold, so that party hold information does not come within the definition of "call-identifying information." See, e.g., US West Comments at 18; USTA Comments at 15. This argument fails for the same reason as does US West's argument about party drops. Like a party drop, a party hold changes the direction and destination of the communications among the remaining parties; the only difference is that a party drop does so permanently, while a party hold does so temporarily.[14]

2. TIA asserts that the J-Standard's Change and Release messages convey substantially the same information that would be captured by the government's proposed party join and party drop messages. TIA Comments at 28-29. We have explained the shortcomings of the Change and Release messages in detail on several previous occasions; rather than repeat ourselves, we refer the Commission to our earlier discussions. See Government June Reply Comments at 51-52; Government December Comments at 46-47; see also Cutright Dec. § B.2.

AT&T asserts that industry "may have more efficient or effective ways than party messages to report joins and drops." AT&T Comments at 10. If so, industry is welcome to use them -- as long as they convey to law enforcement the same information about changes in party status, in the same timely manner, as the proposed party join and party drop messages would convey. However, we note

---

[14] TIA makes the curious assertion that party hold information is "of no relevance to carriers." TIA Comments at 29 n.71. Far from being irrelevant, party hold information is vital for a carrier that is handling a multi-party call. See Cutright Dec. § B.2. If a carrier does not know when a party is placed on hold, the carrier cannot break the party's connection to the call, and if the carrier does not know when the party is taken off hold, the carrier cannot restore the connection.

that AT&T has not identified what these "more efficient or effective" alternatives might be. The Commission should not excuse carriers from providing party join and party drop messages without a specific explanation of alternative solutions and a concrete showing that the alternatives are equally effective.

3. BellSouth asks the Commission to rule that information about the parties to "meet me" conferences (see pp. 33-34 supra) is not "reasonably available" to switch-based CALEA carriers, because such information is "neither used nor generated by the switched network elements in the course of call processing to provide meet-me conference services." BellSouth Comments at 15. This comment assumes that the carrier is using a single intercept access point (IAP) located at the subscriber's switch and that the carrier would have to modify its network to deliver party information from the meet-me conference bridge to that switch. However, a carrier could deliver the party information to law enforcement directly from the network element providing the conference bridge service by adding appropriate IAPs there, eliminating the need to transmit the information from the bridge to the switch.

C. Subject-Initiated Dialing and Signaling Information

The Commission has tentatively concluded that information about a subject's use of flash hooks, feature keys, and similar subject-initiating dialing and signaling activity constitutes "call-identifying information," and that the J-Standard must be modified to require the delivery of such information when it is "reasonably available" to the carrier. Notice ¶¶ 91, 94. The commenters offer a variety of objections to this conclusion, most of which simply repeat arguments that were presented in previous rounds of comments and were rightly found unpersuasive by the Commission.

1. CTIA and PCIA argue that information about a subject's use of hold keys, flash keys, transfer keys, and conference keys does not constitute "call-identifying information." CTIA Comments at 29; PCIA Comments at 27-28. In making this argument, neither CTIA nor PCIA bothers to address the statutory definition of "call-identifying information": "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)). As we have explained before, a subject's use of these feature keys changes the connections between the parties to the call, and in so doing changes the "direction" and "destination" (and in some cases, the "origin" or "termination") of one or more "communication[s] generated or received" by the subject. Moreover, any use of feature keys or flash hooks by a subject to control a call constitutes "direction" of the communications by the subject.[15] As a result, information about the use of these feature keys falls squarely within the definition of call-identifying information. See Government June Reply Comments at 46-48; Government December Comments at 49. Far from relying on a "Wonderland-like interpretation" (CTIA Comments at 29), the Commission's tentative conclusion is supported by a straightforward reading of the statutory definition.[16]

---

[15] Section 103 provides that a carrier's assistance capability obligations apply to all equipment, facilities, and 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 language makes clear that, as used by Congress in Section 103, "direction" encompasses the activity of "directing" a communication, not just the path that the communication follows through the network.

[16] Rather than parse the statutory definition of "call-identifying information," PCIA quotes selected excerpts from the discussion of call-identifying information in the House Report. See PCIA Comments at 27-28. The short response is that the meaning of "call-identifying information" is defined by the statute, not by the House Report. As noted above, the discussion in the House Report has serious limitations as a basis for interpreting the actual definition adopted by Congress. See pp. 22-23 supra.

2. TIA and CTIA argue that the J-Standard's existing call event messages already provide substantially all of the call-identifying information that law enforcement would acquire through the reporting of subject-initiated dialing and signaling activity, and that the only additional information law enforcement would obtain through the reporting of this activity is "the actual keys pressed." TIA Comments at 30-31; CTIA Comments at 27. We have already addressed this argument in our earlier comments, and we refer the Commission to our prior discussion of this issue. As we have explained, it simply is not the case that the only additional information involved here is "the actual keys pressed"; instead, the failure to report subject-initiated dialing and signaling activity will leave serious gaps in law enforcement's ability to understand the course of the subject's communications. See Government June Reply Comments at 48-49; Government December Comments at 49-50.

3. AirTouch and CTIA argue that the use of a feature key to initiate or disable call forwarding does not produce call-identifying information because it "does not directly result in the forwarding of a call," but rather identifies the number to which future calls will be directed. AirTouch Comments at 17; CTIA comments at 28. The definition of "call-identifying information," however, does not distinguish between calls in progress and impending calls. The use of a feature key to activate or deactivate call forwarding "identifies" the "destination" and "termination" of the "communication" to be forwarded, and therefore comes within the scope of CALEA's definition of "call-identifying information." We also note that if law enforcement is not notified that a subject has activated call forwarding at the time that the activation takes place, law enforcement may be unable

to provision the surveillance adequately and may wind up losing call content which it is legally authorized to obtain.[17]

4. BellSouth suggests that the information that law enforcement would derive from a subject's dialing and signaling activity is redundant with the information that law enforcement would learn from party join, party hold, and party drop messages. See BellSouth Comments at 15-16. That is incorrect. Subject-initiated dialing and signaling activity may be either pre-cut-through or post-cut-through, and may be transmitted either in-band or out-of-band. Some of this activity may result in party joins, holds, or drops, but much of it will not. Conversely, there will be many instances in which a change in party connections does not reflect any subject-initiated dialing or signaling activity, such as when one of the other parties on a multi-party call hangs up. In short, while information about subject-initiated dialing and signaling activity may overlap with party join, hold, and drop information in some circumstances, the two categories of call-identifying information are by no means identical.

5. Finally, PCIA notes that, in some switches, the detection and collection of off-hook indicators occurs in a line module that is separate from the main processor of the switch. PCIA suggests that it may be onerous to redesign the switch to send this information from the line module to the main processor for delivery to law enforcement. PCIA Comments at 28. But the line module already must send the off-hook information to the main processor, so that the main processor can act

---

[17] A carrier may make call forwarding available as a usage-based feature, which a subscriber activates as needed by entering the appropriate access code (e.g., *72). Until the subscriber enters the access code, call forwarding is not part of his service package, and law enforcement therefore will not have had any reason to provision the surveillance to be able to intercept forwarded calls. If law enforcement receives immediate notification that call forwarding has been activated, it can act promptly to make the necessary changes in provisioning.

on it in call processing. As a result, PCIA's stated fear about the modifications needed to report off-hook signals is considerably overstated.

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

1. The J-Standard does not provide for the delivery of in-band and out-of-band network signals that identify call progress, such as busy signals, ringing, or call waiting tones. The Commission has tentatively concluded that delivery of certain kinds of in-band and out-of-band network signaling comes within a carrier's assistance capability obligations under Section 103 of CALEA, and has asked for comments regarding the scope of the obligation to deliver network signaling.

The industry comments reflect a persistent, and seemingly willful, misunderstanding of the scope of the network signaling that the government is seeking in this proceeding. First, we are asking a carrier to provide only those signals that are generated (or re-generated) by the carrier's own network. See Government Petition, Appendix 1, § 64.1708(d) ("in-band and out-of-band signaling from the subscriber's service"); Government June Reply Comments at 56-57. We are not asking a carrier to detect and report signaling that "is generated somewhere else and only 'passes through' a network element" of the carrier, as BellSouth suggests (BellSouth Comments at 17).[18] Thus, it simply is not the case that the government's proposal will, for example, require carriers to develop and

[18] CTIA is incorrect when it asserts that the government has departed from this position in the ESS process. CTIA Comments at 30. We have not asked for the delivery of any in-band or out-of-band network signaling that is not generated or regenerated by the carrier's own network.

integrate miscellaneous tone detectors, as Ameritech suggests (Ameritech Comments at 9). A carrier does not need to use tone detectors to "detect" signals that the carrier itself is generating.[19]

Second, we are seeking only network signaling that results in signals that can be sensed by the subject. See Government Petition, Appendix 1, § 64.1708, Table 4. We have no interest in, and are not asking carriers to provide, any network signals that are not perceptible by the subject. For example, a cellular carrier would be under no obligation to provide law enforcement with the many out-of-band signaling messages that are "completely transparent to the user" (AirTouch Comments at 20), such as signaling messages used to control the cellular handset's power levels. Thus, the technical difficulties associated with providing access to such signals are simply irrelevant.

2. In our earlier filings, we have explained why the network signaling at issue here constitutes "call-identifying information." See Government June Reply Comments at 55-56. Several commenters take issue with us on this point, but their remarks largely repeat arguments to which we have already responded.

Nextel asserts that signaling from a carrier to a subject is not call-identifying information because it is not used to "route or process calls through [the] network." Nextel Comments at 13; PCIA Comments at 29. This argument reflects an astonishingly narrow view of what is involved in "process[ing] calls through [the] network." Without network signaling such as ringing, a subject simply will be unaware that an incoming call attempt is taking place, and the calling party will never reach the subject. Providing this kind of network signaling is an integral step in the carrier's

---

[19] TIA asserts that "literally hundreds of features supported by modern switches" involve the kind of in-band and out-of-band signaling sought by the government. TIA Comments at 33. But a variety of different features may employ the same in-band or out-of-band signal. As a result, the number of signals that carriers will be responsible for reporting will be considerably smaller than the number of features that give rise to those signals. See Cutright Dec. § B.4, n.8.

processing of the call, not something unrelated to the task of call processing. Network signaling that reports the progress of outbound calls, such as busy signals, is likewise integral to the carrier's processing of such calls.

SBC asserts that audible network signals, such as ringing, constitute call content rather than call-identifying information, and that law enforcement can obtain such signaling only pursuant to a Title III order. SBC Comments at 14. SBC offers no legal support whatsoever for this radical theory, and none exists. Title III is designed to protect communications between the parties using a telecommunications network, not signaling by the network itself. Cf. 18 U.S.C. § 2510(8) (defining "content" of communications).

Several commenters assert that network notification of waiting voice mail messages (see Notice ¶ 93) is not covered by Section 103 of CALEA because voice mail is an "information service" (47 U.S.C. § 1001(6)) that is outside the scope of CALEA. See Ameritech Comments at 8; Nextel Comments at 14; US West Comments at 21. The commenters are correct that voice mail service is an "information service," and hence "[t]he storage of a message in a voice mail or E-mail 'box' is not covered" by CALEA. House Report at 23, reprinted in 1994 USCCAN at 3503 (emphasis added). But a telecommunications carrier may avail itself of this provision only "insofar as [it is] engaged in providing information services." 47 U.S.C. § 1001(8)(c)(i) (emphasis added). When a telecommunications carrier sends a network notification message to alert the subscriber that he has received a voice mail message, the carrier is acting in its capacity as a telecommunications carrier, not as an information service provider, and therefore the notification message remains within the scope

of the carrier's assistance capability obligations.[20] In this respect, a message-waiting notification signal is no different from the "ping ring" notification that a carrier sends to a subscriber to alert him that an incoming call has been forwarded to another number. FBI Director Freeh's declaration explains the serious problems that lack of access to message-waiting signals causes for law enforcement. See Freeh Dec. ¶ 21(D).

3. Several commenters argue that the J-Standard already provides substantially all of the relevant call-identifying information that would be provided by the reporting of reasonably available in-band and out-of-band network signaling. TIA Comments at 34; PCIA Comments at 29-30; BellSouth Comments at 17. The commenters originally presented this argument in an earlier round of comments, and we have already answered it in detail in our own comments. See Government June Reply Comments at 57-59. For reasons set out there, there are many circumstances in which the J-Standard's existing messages, such as the TerminationAttempt message, will not provide law enforcement with knowledge of the network signaling presented to the subject.

E. Timing Requirements

1. Section 103(a)(2) of CALEA obligates carriers to provide law enforcement with access to call-identifying information "before, during, or immediately after the transmission of a wire or electronic communication," and "in a manner that allows it to be associated with the communication to which it pertains." 47 U.S.C. § 1002(a)(2)(A)-(B). The Commission has tentatively concluded that, in order to satisfy this requirement, the J-Standard must be modified to require carriers to deliver

---

[20] Bell Atlantic suggests that a voice mail notification message constitutes call content. See Bell Atlantic Comments at 10. That suggestion rests on the same logic as SBC's suggestion that all audible notification signals are call content, and it is wrong for the same reasons.

call-identifying information within a "reasonable amount of time" and to "stamp" call-identifying information with the time of the underlying call event. Notice ¶ 104.

Several commenters, including TIA, claim that the J-Standard already obligates carriers to deliver call-identifying information "expeditiously." See, e.g., TIA Comments at 36. Unfortunately, however, it does not. When the J-Standard sets forth obligatory requirements, it uses mandatory language, such as "must" or "shall." See, e.g., J-STD-025, § 4.4 ("The IAP shall access the call-identifying information * * * unobtrusively") (emphasis added). The language in the J-Standard to which the commenters point, in contrast, simply states that "[t]he Call-Identifying Information IAP * * * provides expeditious access to the reasonably available call-identifying information * * * ." J-STD-025, § 4.4. This language is merely descriptive, not prescriptive; it describes the operation of the call-identifying information IAP without purporting to impose any binding obligations regarding delivery time. A carrier therefore can comply with the J-Standard even if it does not deliver call-identifying information "expeditiously." If the J-Standard did implicitly require "expeditious" delivery of call-identifying information, then TIA presumably would have no objection if the Commission were to make that obligation explicit rather than implicit.

2. The government has proposed that call event messages be delivered within 3 seconds 99 percent of the time and that time stamps be accurate to within 100 milliseconds. Although the commenters stop short of endorsing these specific timing requirements, their comments generally acknowledge that timing values comparable to the ones proposed by the government are feasible. See, e.g., TIA Comments at 36-37.

Several commenters suggest that industry and law enforcement have reached a working consensus regarding timing requirements through the ESS process. See, e.g., BellSouth Comments

at 18; CTIA Comments at 31. In its current form, the ESS draft document sets forth separate timing requirements for each call-identifying information message, most but not all of which call for delivery within 3 seconds, and the draft further provides that time stamps shall be precise to within 100 milliseconds. See PN-4177 Working Document Revision 12, §§ 4.2.5.1, 4.2.5.2. These proposed values strongly confirm the feasibility of our own proposed timing requirements. However, the Commission should be aware that the ESS document is a working draft that has not been balloted, and the timing provisions in the document are subject to change. As a more general matter, the Commission should also be aware that the ESS process itself has come under attack by industry in recent weeks -- a development that we discuss further below in connection with the Commission's proposal to leave the drafting of revised standards to TIA. See p. 75 infra. As a result, the Commission should not reach the mistaken conclusion that "consensus" between industry and law enforcement about timing issues has eliminated the need for Commission action.

3. The industry comments raise several specific technical questions relating to the timing requirements proposed by the government. First, AirTouch and SBC suggest that it will be difficult, if not impossible, to ensure that time stamps are synchronized throughout a carrier's network. See AirTouch Comments at 21; SBC Comments at 15. As we have made clear in our previous comments, however, we are not asking for this kind of synchronization. See Government June Reply Comments at 65-66. As a result, its feasibility is irrelevant.

Second, SBC suggests that imposing "strict" time stamping requirements could lead to a loss of call content. SBC Comments at 15. This suggestion is simply incorrect. Neither the application of a time stamp to a call event message nor the precision of the time stamp has any effect on the delivery of call content. Conventional switches are capable of setting up roughly 360,000 calls per

hour and can begin transmitting a message within 10 microseconds. Given these speeds, the process of adding a time stamp to call event messages will not prevent a switch from performing call setup tasks in a timely manner. See Cutright Dec. § B.8.

Third, AT&T suggests that the 3-second delivery requirement should apply to "the first bit of a timing message measured at the point of demarcation between the carrier network and law enforcement's collection facilities." AT&T Comments at 15. We have no objection to this suggestion. The carrier is not responsible for any delays in delivery beyond the demarcation point; as long as the message is delivered to the demarcation point within 3 seconds, the delivery time beyond that point is law enforcement's responsibility.

4. AirTouch (at 21) and SBC (at 15) assert that the adoption of specific timing requirements by the Commission would violate Section 103(b)(1)(A) of CALEA, which provides that CALEA "does not authorize any law enforcement agency or officer * * * to require any specific design of equipment, facilities, services, features, or system configurations to be adopted by any provider of a wire or electronic communication service * * * ." 47 U.S.C. § 1002(b)(1)(A). It is doubtful whether this provision applies to the Commission's actions in this proceeding, since the Commission is not conventionally regarded as a "law enforcement agency." In any event, the Commission is not being asked to "require any specific design of equipment, facilities, services, features, or system configurations * * * ." The timing requirements suggested by the government constitute a performance standard, not a design standard; the Commission is not being called on to prescribe "any specific design" by which the timing requirements are to be met. Finally, the Commission's modifications to the J-Standard, like the J-Standard itself, will constitute a voluntary standard that carriers are not obligated to follow if they are able to satisfy the underlying requirements of Section

103 by other means. See Government May Comments at 14-15. As a result, the Commission will not be, in the language of Section 103(b)(1)(A), "requiring" anything by adding specific timing provisions to the J-Standard.

F. Surveillance Integrity

The government has asked the Commission to modify the J-Standard to incorporate several capabilities relating to surveillance integrity. The Commission has tentatively concluded that these capabilities are not required by Section 103 of CALEA. In our most recent comments, we have asked the Commission to revisit that conclusion. See Government December Comments at 58-66. As we explained there, whether or not CALEA requires the specific surveillance integrity measures proposed in the government's rulemaking petition, it manifestly imposes a general obligation on the part of carriers to take affirmative steps to ensure the integrity of ongoing surveillance, and the J-Standard is deficient because it excuses carriers from taking any such steps.

Because the Commission has tentatively declined to add the proposed surveillance integrity capabilities to the J-Standard, the other commenters devote relatively little attention to them. Nevertheless, the commenters do make several points that call for a response.

1. PCIA and TIA argue that implementing automated surveillance status messages would require wireless carriers to engage in a fundamental redesign of their networks, because wireless networks are not currently configured to poll remote switches to ensure that they are operational and properly configured for surveillance purposes. PCIA Comments at 19; TIA Comments at 38. This argument rests on the assumption that the reporting of surveillance status messages would require a centralized implementation. But rather than polling each network element from a centralized location, a wireless carrier would be free to transmit surveillance status messages directly from each

network element involved in the surveillance, just as each switch will separately transmit call-identifying information and call content to law enforcement. Redesigning the network to provide for centralized polling would not be required; the choice between a centralized approach and a decentralized one is left to the carriers and their vendors. See Cutright Dec. § B.5.

US West suggests that automated surveillance status reporting is unnecessary because law enforcement, not the carrier, "typically" is "the first to become aware of any problem with a wiretap." US West Comments at 22. What US West overlooks is that as electronic surveillance migrates from the local loop to the switch, it becomes far more difficult for law enforcement to "become aware" of a problem in the first place. That is, indeed, the very reason why we have asked for the delivery of surveillance status messages. When law enforcement carries out traditional electronic surveillance over the local loop, it has physical access to the subscriber's line and can confirm for itself that the surveillance is operating and is directed at the right subscriber. See Yarbrough Dec. ¶ 43. When surveillance becomes switch-based, law enforcement no longer has physical access to the interception site and loses its former capability to determine directly the status of the surveillance. Thus, under CALEA, law enforcement must rely on the carrier to take affirmative steps -- either by automated surveillance status reporting or by some other means -- to ensure that the surveillance is operating properly. Id. ¶¶ 44, 47. In the context of cellular communications, law enforcement has already experienced losses of authorized surveillance information because of the failure of carriers to take such steps.

2. PCIA asserts that delivery of an automated continuity check would require carriers to install C-tone generators at the switch level. PCIA Comments at 20. That is incorrect. A C-tone is one form of continuity check, but it is not the only form that would be acceptable. As we have

explained before, we have no objection to the use of existing tones or idle patterns, and we would accept the use of any tones or patterns already in use by the network that could match the functionality of the continuity check described in the government's rulemaking petition. See Government June Reply Comments at 69.

3. PCIA asserts that implementation of an automated feature status message would be infeasible because carriers "do not maintain a real-time database of which features have been implemented by which subscriber at any given time." PCIA Comments at 21. If this were true, it is hard to understand how a carrier could provide service to its subscribers. When a subscriber attempts to invoke a particular feature, such as call forwarding or three-way calling, the network's first task is to determine -- in real time -- whether the feature is available to the subscriber. See Cutright Dec. § B.5. The proposed feature status message therefore does not require the network to detect and report feature status information that is not already available to the network.

G. Post-Cut-Through Dialing

1. One of the principal deficiencies in the J-Standard is its failure to require originating carriers to deliver digits that are dialed by the calling party "post-cut-through" to reach the person with whom the calling party wishes to speak. The Commission has tentatively concluded that "post-cut-through digits representing all telephone numbers needed to route a call * * * are call-identifying information," and therefore must be provided to law enforcement when they are reasonably available to the carrier. Notice ¶ 128. For reasons that we have set forth previously, this conclusion is correct. See Government June Reply Comments at 38-41; Government December Comments at 66-67. Nevertheless, many commenters take issue with it.

The commenters' principal argument is that post-cut-through dialed digits do not constitute call-identifying information "for," or "with respect to," originating carriers. We have already addressed this argument above, in connection with our general discussion of the obligation to provide access to call-identifying information. As explained above, the statutory definition of "call-identifying information" encompasses all dialing and signaling information that "identifies the * * * destination" of "each communication generated or received by a subscriber" (47 U.S.C. § 1001(2)), regardless of whether the particular carrier from whom the information is being sought uses the information for call routing purposes. As a result, the fact that an originating carrier does not use post-cut-through digits to route the call through its network is simply irrelevant. See pp. 23-25 supra.[21]

Nextel argues that "call-identifying information pertains only to 'the equipment, facilities, or services of a subscriber of such carrier,' not to subsequent LECs or IXCs." Nextel Comments at 18 (emphasis in original). But the language that Nextel is quoting comes not from Section 103(a)(2), the assistance capability provision governing call-identifying information, but instead from Section 103(a)(1), the provision concerning delivery of call content. Moreover, Section 103(a)(1) itself sweeps more broadly than Nextel tries to suggest. It encompasses "all wire and electronic communications" carried by a carrier to or from its subscribers' equipment, facilities, or services (47 U.S.C. § 1002(a)(1) (emphasis added)), and therefore unquestionably includes communications

---

[21] For this reason, it is immaterial that cellular and PCS systems do not use DTMF audio digits for call routing purposes, as AirTouch argues. See AirTouch Comments at 25-26. If a cellular or PCS subscriber engages in post-cut-through dialing on a mobile handset to complete a call, the dialed digits constitute "call-identifying information" regardless of how the cellular or PCS carrier treats the digits, because they "identify the * * * destination" of a "communication generated or received by [the] subscriber."

between a subscriber and a called party after the cut-through takes place.[22] As a result, even if a carrier's obligation to deliver call-identifying information under Section 103(a)(2) were expressly confined to information about communications covered by Section 103(a)(1) (and it is not), that obligation would still encompass the post-cut-through digits dialed by the subscriber to reach the called party.

EPIC suggests that if post-cut-through dialed digits constitute "call-identifying information," as the government contends, then so would the words spoken by a subject who orally gives a telephone number to a long-distance operator. EPIC Comments at 32. This reductio ad absurdum is incorrect. The definition of call-identifying information is confined to "dialing or signaling information" (47 U.S.C. § 1001(2) (emphasis added)), and words spoken by one person to another do not constitute "dialing or signaling information."[23]

2. EPIC, along with other commenters, points out that a subject may engage in post-cut-through dialing for purposes other than call completion, such as sending instructions to an automated bank account or entering a credit card number. EPIC Comments at 28. EPIC argues that post-cut-through digits entered for such purposes do not constitute call-identifying information. We agree. Contrary to EPIC's claim, we are not trying to stretch the definition of "call-identifying information"

---

[22] As the Commission has noted in other settings, "a 'completed' call is a call that is answered by the called party." Report and Order, In re Implementation of the Pay Telephone Reclassification and Compensation Provisions of the Telecommunications Act of 1996, Docket No. 96-388 (released Sept. 20, 1996), at 33. Thus, when a subscriber calls another party by using an "800" long-distance service, the subscriber's call is not completed until it reaches the called party.

[23] This does not imply that law enforcement would necessarily have to obtain a Title III interception order to obtain access to phone numbers conveyed orally to an operator. See Smith v. Maryland, 442 U.S. 735, 744 (1978) (indicating that subject who "placed his calls through an operator" would have "no legitimate expectation of privacy" in the words spoken to the operator).

to encompass post-cut-through dialing that is used for purposes other than call routing. See Government June Reply Comments at 39. Our position is simply that when post-cut-through dialing is performed in order to complete a call, it constitutes call-identifying information, and it therefore comes within the scope of the carrier's obligations under Section 103(a)(2) of CALEA.[24] In these circumstances, the only real issue is how to meet law enforcement's minimization obligations, not whether law enforcement should be provided with access to the information in the first place.

If a carrier has the technical capability to distinguish automatically between post-cut-through digits used for call completion and post-cut-through digits entered for other purposes, the carrier is free to employ that capability to give law enforcement only the digits used in call completion. To our knowledge, however, no such technical capability currently exists. See Government December Comments at 67. In the absence of such a capability, the carrier must deliver either all post-cut-through digits or none, and the latter course is inconsistent with the carrier's obligation to provide call-identifying information under Section 103(a)(2). For reasons that we have explained before, nothing in CALEA excuses a carrier from delivering post-cut-through digits that are "call-identifying information" simply because doing so will unavoidably result in the delivery of other post-cut-through digits that are not. See Government June Reply Comments at 40-41.

---

[24] EPIC quotes from a letter from the Department of Justice to Congress regarding proposed "clone pager" legislation. The letter, a copy of which is attached to EPIC's comments, states that "the information transmitted [to a pager] after a phone call is connected to the called party" is "substantive in nature," because it is "not used to direct or process the call, but instead [to] convey certain messages to the recipient." Letter from Acting Assistant Attorney General Ann M. Harkins to the Hon. Henry J. Hyde, May 20, 1998, pp. 2-3 (emphasis added). As the underscored language makes clear, the legal analysis in the Department's letter in no way suggests that dialing activity that takes place before "a call is connected to the called party," for the purpose of "direct[ing] or process[ing] the call," is substantive in nature.

EPIC suggests that when law enforcement receives post-cut-through digits that are not dialed for call routing purposes, it is engaging in an "interception" of communication for purposes of Title III, and therefore must make the heightened showing required to obtain a Title III interception order, rather than relying on a pen register order. See EPIC Comments at 28-29. This argument is incorrect. Congress placed the use of pen registers and trap-and-trace devices outside the scope of Title III altogether. See 18 U.S.C. § 2511(h)(i); see also Smith v. Maryland, 442 U.S. 735 (1979). The pen register statute authorizes law enforcement to acquire all "numbers dialed or otherwise transmitted" by the subject using the monitored facilities (18 U.S.C. § 3127(3)); it does not restrict that authorization to numbers dialed for call processing purposes. Thus, at least as long as a carrier is unable to differentiate between digits dialed for call processing purposes and digits dialed for other purposes, law enforcement may obtain all dialed digits from the carrier pursuant to a pen register order without running afoul of Title III. If the law were otherwise, there would have been no reason for Congress to enact 18 U.S.C. § 3121(c), the pen register statute's minimization provision, which obligates law enforcement to "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." This provision presupposes that law enforcement agencies executing pen register orders can and will receive dialing and signaling information that is not "utilized in call processing," and simply directs that such information not be "record[ed] or decod[ed]" if (and only if) reasonably available technology so permits.[25]

---

[25] AT&T asserts that "[t]here are no provisions in the pen register statute that require minimization." AT&T Comments at 21; Nextel Comments at 20 n.47 (same). This assertion simply overlooks 18 U.S.C. § 3121(c). See House Report at 17, reprinted in 1994 USCCAN at 3497 (CALEA "requires law enforcement to use reasonably available technology to minimize information (continued...)

In a similar vein, several commenters suggest that carriers who provide law enforcement with access to post-cut-through dialed digits might be exposed to legal liability for doing so. See, e.g., Nextel Comments at 20. This suggestion is thoroughly misconceived. Title III expressly states that providers of wire and electronic communication services "are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance," whenever they are provided with an appropriate court order. 18 U.S.C. § 2511(2)(a)(ii). Title III further states that "[n]o cause of action shall lie in any court" against a provider of wire or electronic communications services "for providing information, facilities, or assistance in accordance with the terms of a court order or certification under this chapter." Ibid. The pen register statute likewise states that "[n]o cause of action shall lie in any court" against a provider of wire or electronic communication services "for providing information, facilities, or assistance in accordance with the terms of a court order" under the pen register statute. Id. § 3124(d). Finally, Title III and the pen register statute both provide that "good faith reliance" on a court order or other legal authorization is "a complete defense against any civil or criminal action" brought under Title III, the pen register statute, or any other law. Id. §§ 2520(d)(1), 3124(e). As a result, a carrier that complies with an appropriate court order requiring the carrier to provide access to post-cut-through dialed digits faces no risk of legal liability.

3. TIA and several other commenters argue that law enforcement should not look to the originating carrier for post-cut-through dialed digits, but rather should turn to the carrier that uses the post-cut-through digits to route the call. TIA suggests that if post-cut-through digits can be

---

[25](...continued)
obtained through pen registers").

obtained from other carriers, requiring originating carriers to provide them would be inconsistent with Section 107(b)(1)'s mandate to use "cost-effective methods" for meeting CALEA's assistance capability requirements. TIA Comments at 42.

Unfortunately, the alternative of obtaining post-cut-through digits from other carriers is an illusory one. For reasons that we have discussed at length in our earlier filings, post-cut-through digits cannot be obtained "expeditiously" from other carriers (see 47 U.S.C. § 1002(a)(2)), and often will not be available at all. See Government June Reply Comments at 41-42 & n.24; Government December Comments at 68-69. As a result, law enforcement's request for post-cut-through digits from originating carriers is not a prohibited demand for "one-stop shopping," as the commenters repeatedly suggest (e.g., Bell Atlantic Comments at 10). Instead, it is a matter of practical necessity.

Ameritech and BellSouth suggest that, rather than requiring the originating carrier to detect post-cut-through digits and extract them for delivery on a call data channel (CDC), law enforcement agencies should provision a call content channel (CCC) from the originating carrier's switch and extract the DTMF tones at the collection facility. See Ameritech Comments at 12; BellSouth Comments at 18. Under this proposal, the originating carrier would transmit to law enforcement not only the post-cut-through dialed digits, but also the content of the subject's post-cut-through communications. Ameritech and BellSouth suggest that this approach would be more economical than requiring carriers to modify their equipment to detect post-cut-through dialing.

Apart from the fact that the J-Standard currently does not require the delivery of post-cut-through digits by any means, including delivery over a CCC, there are at least two major problems with this proposal. First, while Ameritech and BellSouth (and other commenters) express concern about the cost of dialed digit extraction for originating carriers, they take no account of the costs

associated with requiring law enforcement to provision CCCs to capture post-cut-through dialing in pen register cases. If post-cut-through digits are extracted by the originating carrier, they can be delivered over the same CDC that is being used to implement the pen register order. But under Ameritech's and BellSouth's proposal, law enforcement would also have to provision at least one CCC in addition to the CDC, and law enforcement would have to do so in every pen register case simply to ensure that it is capable of identifying the parties that the subject is calling.

When law enforcement leases a dedicated line, it typically has to pay an initial setup charge of roughly $700 and an additional payment of $100 per month, although higher prices are not uncommon. This means a cost of roughly $1,000 for a pen register surveillance that lasts three months, a common length of time. In a typical year, the FBI executes pen register and trap-and-trace orders on approximately 10,000 lines, and state and local law enforcement agencies perform a comparable volume of pen register and trap-and-trace surveillance. Thus, the cost entailed in provisioning CCCs for pen register cases could amount to as much as $20 million per year -- each year, year after year. It is understandable that Ameritech and BellSouth do not dwell on these costs, since they represent a source of revenue rather than expense to carriers. But to the extent that the Commission deems cost considerations to be relevant under Section 107(b), the substantial costs of requiring law enforcement to provision CCCs for pen register cases should weigh against this proposal.

Second, as we have pointed out previously, delivering the contents of a subject's post-cut-through communications to law enforcement pursuant to a pen register order poses unnecessary risks to privacy interests. See Government June Reply Comments at 45. We do not mean to suggest, as some commenters do, that the arrangement proposed by Ameritech and BellSouth would exceed the

scope of law enforcement's authority under the pen register statute and could be implemented only pursuant to a Title III order. Nevertheless, it would create a risk that innocent conversations might be heard inadvertently by law enforcement in the course of pen register surveillance. Where it is practical for a carrier to deliver dialing and signaling information to law enforcement without also delivering the contents of the communication, the Commission may take account of privacy concerns in selecting among the alternatives. See 47 U.S.C. § 1006(b)(2).

4. In earlier filings, we have discussed the mechanics of detecting and extracting post-cut-through dialed digits. See Government June Reply Comments at 43; Government December Comments at 67. We have only two points to add in response to the comments of the other parties on this issue. First, the detection of post-cut-through digits does not have to take place inside the switch; it can be performed outside the switch by means of a "loop around" arrangement, and doing so may be both easier and less expensive. See Cutright Dec. § B.7. Second, some wireless switches generate DTMF tones in response to out-of-band messages originating at the wireless handset. Carriers using these switches have no need to install tone decoders at the switch and send the generated tones to law enforcement; instead, they simply can report the messages that cause the switch to generate the tones.

H. Location Information

In certain circumstances, the J-Standard requires carriers to provide law enforcement agencies with location information at the beginning and end of communications to and from mobile terminals. The Commission has tentatively concluded that the location information prescribed by the J-Standard is "call-identifying information" under CALEA. Notice ¶ 52. CDT takes issue with that tentative

conclusion and urges the Commission to remove the location information provisions from the J-Standard. See CDT Comments at 4-12.

In large measure, CDT's arguments about location information reprise CDT's earlier comments in this proceeding. We have addressed those comments in detail in our own previous filings, and we refer the Commission to our earlier discussions for an explanation of the shortcomings in CDT's legal argument. See Government May Comments at 17-21; Government June Reply Comments at 78-79. Nevertheless, several points in CDT's most recent filing call for a further response.

At the outset, it is critical for the Commission to keep in mind that the J-Standard provides for the delivery of location information only when law enforcement has legal authority to obtain such information. Location information is included in J-Standard messages only when "delivery is [legally] authorized." See, e.g., J-STD-025, § 5.4.1, Table 1 (Location parameter, Usage column); see also id. § 5.4 (discussing meaning of "conditional" parameters). The J-Standard does not require the delivery of location information unless law enforcement is acquiring such information pursuant to an appropriate court order or other legal authorization. As a result, the J-Standard creates no risk whatsoever that law enforcement will obtain location information that Congress does not want it to obtain.

CDT nevertheless argues at length that the Commission's tentative conclusion conflicts with "one of the key compromises struck in 1994 when CALEA was being drafted and debated." CDT Comments at 2. This gets the matter exactly backward. CALEA indeed embodies a compromise regarding location information. But it is CDT, not the Commission, that has misunderstood the nature of the compromise.

The legislative compromise regarding location information is written into Section 103(a)(2) of CALEA, in plain and unambiguous terms: "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." 47 U.S.C. § 1002(a)(2) (emphasis added). Congress could hardly have been any clearer about its intent: when law enforcement is proceeding "solely pursuant to the [legal] authority for pen registers and trap and trace devices," carriers are not to treat location information as call-identifying information, but when law enforcement has been duly authorized to acquire location information under other electronic surveillance statutes, location information remains part of call-identifying information.[26] The J-Standard is consistent with this intent; CDT's position is not. See Government May Comments at 18-19.

CDT argues that location information does not come within the scope of call-identifying information because the statutory definition of call-identifying information does not include the term "location." CDT Comments at 5. But the definition does include the terms "origin" and "destination," and as the Commission has noted, those terms readily encompass the location from which a wireless call is being sent or received. See Notice ¶ 52. It may well be true, as CDT says, that "origin" and "destination" have further meanings in addition to location (CDT Comments at 5), but it hardly follows that their meanings exclude location. See, e.g., Oxford English Dictionary,

---

[26] US West asserts that the pen register statute is the only legal basis for acquiring location information, and hence the location proviso of Section 103(a)(2) serves to place location information entirely beyond the reach of law enforcement. US West at 25. That assertion is incorrect. There are at least two other sources of legal authority under which law enforcement may, upon a proper showing, obtain location information: an interception order under Title III, 18 U.S.C. §§ 2510 et seq., and an order for the disclosure of customer records under 18 U.S.C. § 2703(c)-(d). CDT, unlike US West, makes no claim that the pen register statute is the sole source of authority for this information.

Compact Edition 702 (1971) ("destination" means, inter alia, "the place for which a person or thing is destined"); id. at 2010 (giving examples of the use of "origin" to signify location). Moreover, if "origin" and "destination" are read to exclude location information altogether, as CDT urges, then the location proviso in Section 103(a)(2) becomes superfluous, CDT's claims to the contrary notwithstanding.

It is not the case, as CDT suggests, that the Commission's reading of "origin" and "destination" gives those terms different meanings for wireless and wireline communications. The terms encompass location both in the wireless setting and the wireline setting. In the case of wireline communications, however, the fixed location of the subscriber's terminal means that the number of the party using the terminal identifies the location of the call, so no separate location information is required.[27]

Finally, CDT conspicuously fails to explain why Congress would have intended to exclude location information from the scope of CALEA altogether, even in circumstances where it is uncontested that law enforcement has full legal authority to obtain such information. CDT argues that information about the location of a wireless handset is more invasive than information about the location of a wireline terminal because the user of a wireless handset "almost always is the individual subscriber" (CDT Comments at 12), so that law enforcement learns not only where the call is coming from but also who is speaking. CDT's assumptions about who uses wireless handsets are debatable: wireless handsets may be used by many persons other than individual subscribers, such as a

---

[27] CDT asserts that the Commission's reading of "origin" and "destination" does not explain why the J-Standard provides location information at the end of an outgoing call. CDT Comments at 6. The explanation is that the location of the mobile handset identifies the "origin" of the communication regardless of whether the communication is beginning or ending.

subscriber's family members and colleagues, and in the case of corporate usage (which accounts for a substantial share of wireless traffic), the user could be any one of hundreds or even thousands of a corporate subscriber's employees. In any event, CDT's real argument here is not with the Commission but with Congress, for the J-Standard provides access to location information only when laws other than CALEA authorize law enforcement to obtain such information. To the extent that CDT has concerns about the privacy implications of those laws, its recourse lies outside the confines of this proceeding.

I. Packet Mode Communications

1. From the outset of this rulemaking proceeding, CDT has taken issue with Section 4.5.2 of the J-Standard, which permits carriers transmitting packet mode communications to send law enforcement the entire packet data stream associated with a given communication, including the content of the communication as well as the associated call-identifying information in the packet header. See J-STD-025 § 4.5.2, ¶ 2 (Packet Data IAP). In our earlier comments, we have explained why this provision of the J-Standard is consistent with the assistance capability requirements of CALEA. See Government May Comments at 21-22; Government December Comments at 77-80. As we have explained, in pen register cases, 18 U.S.C. § 3121(c) obligates law enforcement to "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." Technology is currently available to law enforcement that distinguishes between a packet's header and its communications payload and makes only the relevant header information available for "recording or decoding." The J-Standard relies on law enforcement to comply with its legal obligations under 18 U.S.C. § 3121(c)

in this fashion, and nothing in Section 103(a) -- or any other provision of CALEA -- prohibits this arrangement.

In its latest comments, CDT elaborates on its proposed alternative to the J-Standard's current packet data delivery provision. CDT argues that Section 103(a)(2) of CALEA obligates a carrier only to provide law enforcement with the information in a packet that the carrier itself uses to route the communication, and that the carrier is under no obligation to deliver information in the packet that is used for routing purposes by other carriers who are "upstream" or "downstream" in the data transmission path. CDT proposes that "any carrier using packet technologies should disclose pursuant to a pen register order the transactional information that it uses to process communications," and should not be required to provide "the transactional information used by other carriers." Id. at 13 (emphasis in original). Thus, when a packet is transmitted across the networks of (for example) four different carriers, law enforcement should (under CDT's proposal) ask each carrier separately for the information in the packet header that that carrier uses in routing the communication.

This proposal has profound problems, both legally and practically. If the Commission were to adopt it, law enforcement's electronic surveillance capabilities in cases involving packet mode communications would be severely compromised.

We have already identified the basic legal shortcoming of CDT's position in connection with our general discussion of call-identifying information. See pp. 23-25 supra. As we explained there, CDT's position rests on the proposition that "call-identifying information" is a "subjective" or "relative" concept, meaning that the status of information as "call-identifying information" depends on the use to which a particular carrier puts it. Under this view, information changes back and forth

from call-identifying information to call content as it passes between a carrier that uses it for call routing purposes and a carrier that does not. See CDT Comments at 21-22.

The problem with this argument is that, as we have explained above, it simply cannot be squared with CALEA's definition of "call-identifying information." Particular information in a packet header either does or does not "identif[y] the origin, direction, destination, or termination" of a "communication generated or received by [the] subscriber." 47 U.S.C. § 1001(2). If it does, it is "call-identifying information" -- period. It does not flicker back and forth spectrally from one state to another, like Marley's ghost.[28]

Not only is CDT's position legally unsupportable, but it presents fundamental practical problems as well. CDT's proposal would require law enforcement to seek information from every carrier in the packet data stream in order to determine the origin and destination of a single packet mode communication. In many instances, law enforcement would have no way of knowing in advance which "downstream" carriers would wind up handling the communication after the packet stream passes through the hands of the originating carrier. Law enforcement therefore would be unable to identify the destination of an outgoing communication at the time that it takes place, and would never be able to identify the destination if, as ordinarily will be the case, the downstream carrier does not retain a record of the call-identifying information in the packet header after the communication is complete.

---

[28] "Scrooge, having his key in the lock of the door, saw in the knocker, without its undergoing any intermediate process of change -- not a knocker, but Marley's face. * * * As Scrooge looked fixedly at this phenomenon, it was a knocker again." Charles Dickens, A Christmas Carol 23 (1991 ed.).

Moreover, in many instances, CDT's proposal would require law enforcement to serve pen register orders on Internet service providers (ISPs). See CDT Comments at 16. To the extent that ISPs are engaged in providing "information services" (47 U.S.C. § 1001(6), (8)(c)(i)), they are outside the scope of CALEA's assistance capability requirements. See House Report at 18, reprinted in 1994 USCCAN at 3498. Thus, the effect of CDT's proposal -- and, it is fair to assume, CDT's underlying purpose -- is to diminish law enforcement's access to call-identifying information that it is legally authorized to acquire, by forcing law enforcement to turn from telecommunications carriers who are subject to CALEA's assistance capability requirements to information service providers who are not.

The fundamental object of CALEA is to narrow the gap between law enforcement's legal authority to conduct electronic surveillance and its technical capability to exercise that authority. CDT's proposal would have precisely the opposite effect: it would expand that gap rather than narrow it. CDT's proposal thus strikes at the heart of Congress's goals in enacting CALEA. The Commission must not permit Congress's objectives to be undermined in this fashion.

2. Bell Atlantic Mobile urges the Commission "to declare as part of any capability rule that the rule does not apply to packet transmissions," such as those handled by Bell Atlantic Mobile's Cellular Digital Packet Data network. Bell Atlantic Mobile Comments at 12. This suggestion is misconceived. As explained in our prior comments, CALEA does not distinguish between packet mode and circuit mode communications. See Government December Comments at 81-82. The assistance capability requirements of Section 103(a) of CALEA apply to all "telecommunications carriers" and encompass all "wire and electronic communications" carried by such carriers. 47 U.S.C. § 1002(a)(1)-(2). If a telecommunications carrier is transmitting a "wire communication" or an

"electronic communication," as those terms are defined (18 U.S.C. § 2510(1), (12)), the carrier must comply with Section 103 with respect to those communications, regardless of whether the carrier is using packet mode technology or some other technology to transit the communications. Like CALEA itself, the J-Standard encompasses packet mode as well as circuit mode communications, and the Commission's final Report and Order should do likewise.

3. Metricom argues that carriers should not be required to provide law enforcement with access to wireless packet-mode data, because such data are typically encrypted by users in ways that, according to Metricom, "make meaningful interception of call content impossible." Metricom Comments at 2-4. The short answer to this argument is that CALEA does not relieve carriers from their obligation to provide access to call content (47 U.S.C. § 1002(a)(1)) when a communication is encrypted. Instead, CALEA provides that "[a] telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication." 47 U.S.C. § 1002(b)(3). As this provision indicates, Congress was well aware that particular communications might be encrypted. Its response was assign responsibility for decryption to law enforcement, not to release carriers from the duty to deliver encrypted communications to law enforcement in the first instance.

III. Comments Regarding Implementation Issues

A. Revision of J-Standard

1. In our earlier comments, we addressed the Commission's proposal to assign the TIA standard-setting committee responsible for the J-Standard with the task of preparing new technical standards that correct the deficiencies in the J-Standard identified by the Commission. See

Government December Comments at 30-34. In some respects, the comments submitted by the other commenters make the same points that we have made, such as the importance of giving TIA precise "marching orders" in order to minimize confusion and disagreement about its goals. In other respects, however, the commenters have a different view about the course that a remand should follow.

The principal disagreement concerns how long the process of revising the J-Standard should take. The Commission's Notice proposes that TIA "complete any such modifications * * * within 180 days of release of the Report and Order in this proceeding." Notice ¶ 133. We endorse that timetable. However, TIA argues that it will take 180 days simply to prepare draft standards for balloting, and that an additional 3 to 5 months should be permitted for the balloting process. TIA Comments at 3, 13, 15. TIA thus asks the Commission to allow as much as 11 months for redrafting the J-Standard, and other commenters ask for even more time. See, e.g., US West Comments at 30-31 (14 to 17 months).

We urge the Commission to adhere to its proposal that the revision process be completed within 180 days, not simply to provide for the commencement of balloting within that time. TIA's proposed timetable reflects a "business as usual" approach, in which committee meetings are scheduled on a relatively infrequent and episodic basis. If the Commission intends to enlist the aid of industry in revising the J-Standard, rather than performing that task itself, TIA's business-as-usual approach must give way to the need to implement CALEA's assistance capability requirements as soon as possible. Congress's goal of preserving law enforcement's ability to carry out legally authorized surveillance should not be undermined by further delays in the implementation process.

If the Commission is specific about the changes required in the J-Standard, there is no reason why the parties cannot produce a ballot-ready draft within 90 days, which would allow an additional

90 days if necessary for balloting and post-ballot revisions. As noted in our prior comments, law enforcement and industry have been engaged in ongoing discussions for the past year, under the aegis of TR45.2's ESS (Enhanced Surveillance Services) project, about technical standards that would implement the capabilities at issue in this proceeding. As a result of that process, TIA would not be starting from scratch, but rather could draw on the substantial efforts and progress already made in defining the added assistance capabilities.

In recent weeks, industry has threatened to terminate the ESS project, while suggesting that law enforcement rather than industry is responsible for the failure to complete the process. The timing of industry's action, coming when the Commission is deciding how much time will be required to revise the J-Standard, strongly suggests that industry is trying to minimize the progress already made by the ESS project in order to justify a longer "remand" period. The government has made clear to industry that we strongly support the work produced by the ESS project. If industry nevertheless chooses, for its own reasons, to discontinue the ESS project, the Commission should not allow industry to reap the benefits by extending the time for implementing the Commission's decision and order. Indeed, if industry is serious about abandoning the ESS project, the Commission may well need to reconsider whether TIA should be entrusted at all with the task of implementing the Commission's changes to the J-Standard.

Industry's threat to walk away from the ESS process also underscores the need for the Commission to monitor the remand process to ensure that TIA meets the deadlines set by the Commission. In addition to designating Commission staff members to attend the standards meetings as observers (Government December Comments at 33-34), the Commission may also wish to require periodic status reports from TIA. If the Commission sees that its deadlines are not going to be met,

it should accept proposed technical standards from law enforcement as a basis for further proceedings before the Commission. See Government December Comments at 33.

B. Compliance Deadline

1. The other major issue relating to implementation is the deadline for compliance with the assistance capabilities that the Commission adds to the J-Standard. In our comments, we suggested that the Commission require compliance no later than 18 months after the revisions to the J-Standard are complete. If the revision process takes 180 days, that would mean a compliance deadline of 24 months after the Commission's report and order. See Government December Comments at 29-30. Thus, if the Commission were to issue its report and order in the second quarter of 1999, compliance would be required by the second quarter of 2001.

Predictably, most (although not all) of the industry commenters argue for a far later compliance deadline. TIA suggests that compliance with the added capability requirements be deferred until June 2003 -- more than four years from now. TIA Comments at 2, 18. Other commenters propose similarly extended compliance deadlines. See, e.g., AirTouch Comments at 28; GTE Comments at 14-15.

TIA suggests that a prolonged implementation timetable is necessary because most manufacturers "will not be able to begin their design and development work" on the revisions to the J-Standard "until development and installation of the 'core' J-STD-025 features is complete." TIA Comments at 18. We believe, however, that many manufacturers already have engineers working on the design and development of CALEA solutions that include law enforcement's punch list items. Moreover, the engineers who are responsible for designing software ordinarily are assigned to new projects at the beginning of the testing phase. As a result, TIA's scenario, in which manufacturers

cannot begin to deal with the punch list items until they are finished with the core J-Standard capabilities, does not provide an accurate picture of how the development process will work.

Several commenters argue that implementing modifications to the J-Standard will jeopardize other industry tasks, such as dealing with the "Y2K" problem, Local Number Portability, the E911 initiative, and so forth. We do not mean to disparage these other initiatives, all of which are important in their own right. Nevertheless, the suggestion that implementing the Commission's order "may be the straw that breaks the regulatory camel's back" (CTIA Comments at 18) has an air of hyperbole about it. If the need to deal with issues like Y2K, LNP, and E911 has not prevented industry from continuing to develop and implement new features and services for their customers; neither should it excuse industry from taking the steps needed to meet its statutory obligations under CALEA. We do not share the industry commenters' apparent view that the interests served by CALEA must take a back seat to other industry concerns. What is at stake in this proceeding is law enforcement's ability to use legally authorized electronic surveillance to protect the public safety and security by detecting, preventing, and prosecuting criminal activities. These are interests of paramount importance, as the declarations of FBI Director Freeh and DEA Administrator Constantine underscore, and they should not be consigned to second-class status in the allocation of industry resources.

2. Several commenters argue not only that the Commission should allow a lengthy period for implementation of the new assistance capabilities, but that the current, already-extended deadline for implementation of the J-Standard -- June 30, 2000 -- should be extended yet again to coincide with the deadline for the new capabilities. See, e.g., CTIA Comments at 19; Nextel Comments at 25; Bell Atlantic Mobile Comments at 13-14. These commenters suggest that a single (and, needless to say,

late) compliance deadline would be more "efficient" than separate deadlines for the core J-Standard and the capabilities that are added in this proceeding.

When the Commission issued its order in September 1998 granting an industry-wide extension of the date by which the obligations of Section 103 will become effective, the Commission stressed that the new deadline of June 30, 2000, was a "firm" one. Extension Order ¶ 46. It is hardly surprising, but nevertheless regrettable, that the industry is already inviting the Commission to abandon that deadline in favor of a substantially later one. We urge the Commission to reject this invitation and reiterate that the existing deadline is a firm one that will not be changed.

The current industry comments indicate that while individual carriers may encounter obstacles in meeting the June 2000 deadline, there is no reason to think that the industry as a whole will be unable to meet that deadline. For example, TIA states that "[w]ireline, cellular and broadband PCS manufacturers are working closely to comply with the Commission's extension of the compliance deadline for the 'core' J-STD-025," and suggests that only "individual" petitions for extension may be necessary. TIA Comments at 19 n.42. No commenter even attempts to argue that compliance with the June 2000 deadline is beyond the reach of all carriers. As a result, the Commission should make clear that any requests to extend the current deadline will be entertained only on a carrier-specific rather than industry-wide basis.[29]

The suggestion that it would be more "efficient" to have a single compliance deadline is inconsistent with our understanding of how manufacturers expect to provide their CALEA solutions

---

[29] GTE suggests that the Commission give the Chief of the Common Carrier Bureau authority to grant nine-month extensions of the implementation deadline, based on showings of "need" by individual carriers. GTE Comments at 16. However, CALEA provides that requests for extensions will be acted on by the Commission itself, in "consultation with the Attorney General," rather than being delegated to one of the Commission's bureaus. 47 U.S.C. § 1006(c)(2).

to carriers. We understand that manufacturers generally intend to rely on a phased deployment, in which CALEA capabilities are made available over a series of several generic upgrades. Having one deadline for the "core" J-Standard capabilities and a subsequent deadline for the additional capabilities is consistent with this phased deployment model.

Moreover, the suggestion that the Commission delay the deadline for implementing the J-Standard takes no account whatsoever of the law enforcement requirements that underlie CALEA. Congress enacted CALEA in 1994. Even with the existing deadline, wireline and cellular/PCS carriers will not implement the core J-Standard until mid-2000, nearly 6 years after CALEA was enacted. The technical obstacles to electronic surveillance that led Congress to enact CALEA in 1994 are no less pressing today than they were then; to the contrary, they grow more pressing every day. To extend the compliance deadline yet again would compound law enforcement's growing inability to employ authorized electronic surveillance of modern telecommunications networks to protect public safety and security. The public has a vital interest in seeing that the Commission avoid that result.

DATE: January 27, 1999

Respectfully submitted,

Louis J. Freeh, Director
Federal Bureau of Investigation

Honorable Janet Reno
Attorney General of the United States

Donald Remy
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

I, David Yarbrough, a Supervisory Special Agent in the office of the Federal Bureau of Investigation (FBI), Washington, D.C., hereby certify that, on January 27, 1999, I caused to be served, by first-class mail, postage prepaid (or by hand where noted) copies of the above-referenced Reply Comments Regarding Further Notice of Proposed Rulemaking, the original of which is filed herewith and upon the parties identified on the attached service list.

DATED at Washington, D.C. this 27th day of January, 1999.

_____
David Yarbrough