

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

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

REPLY COMMENTS OF THE NEW YORK CITY POLICE DEPARTMENT
REGARDING FURTHER NOTICE OF PROPOSED RULEMAKING

John Pignataro
Sergeant Detective Supervisor
Electronic Surveillance Technical Advisor
New York City Police Department
Building 610, Fort Totten
Bayside, New York 11359
(718) 971-1408

Edward T. Norris
Deputy Commissioner, Operations
New York City Police Department
1 Police Plaza, Room 910
New York, New York 10038
(212) 374-6100

SUMMARY

The New York City Police Department (NYPD) submits these reply comments regarding the Further Notice of Proposed Rulemaking released by the Federal Communications Commission ("Commission") on November 2, 1998, for the implementation of the Communications Assistance for Law Enforcement Act (CALEA). These reply comments respond to comments submitted by December 14, 1998, by various interested parties. NYPD also supports the reply comments submitted in this matter by the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI).

NYPD seeks to direct the discussion surrounding CALEA implementation to the original intent of the statute. In particular, the parties to this proceeding have, in NYPD's opinion, lost sight of the Congress' unequivocal guarantees that law enforcement will continue to have access to information that has historically been included in the category of legally authorized electronic surveillance.

If implemented according to the legislative intent, CALEA will allow law enforcement, upon receipt of a legally issued order, to obtain information generated by the calling activities of criminal suspects regardless of the telecommunications technology used and, even more importantly, regardless of the telecommunications carrier that provides the suspect with service.

NYPD has frequently observed that criminals intentionally use telecommunications services that are known to be impediments to surveillance technology. Any CALEA solution implemented must stop this practice by ensuring that, pursuant to a court order, law enforcement can receive information from all carriers.

NYPD believes that the current industry interim technical standard is deficient. This interim standard lacks capabilities that are essential to law enforcement's continued effective use of lawfully authorized electronic surveillance as an investigative tool. Lawfully authorized electronic surveillance is a key investigative method used by law enforcement. Without the requisite capability to conduct lawfully authorized electronic surveillance commensurate with statutory authority, law enforcement's mission of protecting the public and ensuring its safety will be greatly impeded.

Lawfully-authorized electronic surveillance is being used on a more frequent basis by NYPD because criminal sophistication is rising and other investigatory methods do not allow for safe and effective means of collecting evidence. There has also been a noticeable increase in the number of failed intercept attempts because telecommunications technologies and services is far out-stripping our attempts to conduct lawfully-authorized electronic surveillance. NYPD believes that the Commission should incorporate *all* nine of the missing assistance capabilities that the DOJ/FBI have determined to be within the statutory framework of Section 103 of CALEA.

communications and advances in telecommunications technology did not disturb the *status quo*.

2. Some commenters argue that including the punch list items in a CALEA solution will expand the category of information law enforcement has received in the past.² In reality, the punch list items are necessary to maintain the *status quo*. For example, "call forwarding," a common feature used today by many subscribers, illustrates this point. In the past, law enforcement could obtain call-identifying information that showed, for example, the number to which a criminal suspect forwarded his or her calls. Every time a subscriber wished to change the number to which calls were forwarded, the subscriber employed a vertical service code from the subscriber's phone that was discernable to law enforcement. In the case of call forwarding, star 72 (*72) was used to activate the feature. Law enforcement received both the star code, which indicated that the call forwarding feature was being activated, and the number to which the call was sent. Today, however, customers can set up and change call forwarding options from any phone. This development results in a significant loss to law enforcement by providing criminals with a simple way to circumvent a lawfully obtained court order. Contrary to the arguments of commenters,³ this is precisely the type of loophole Congress intended to close by passing CALEA.

² See, e.g., Bell Atlantic at 1, 2-4; GTE at 2.

³ See, e.g., EPIC/EFF/ACLU at 25 ("Congress did not intend to define as call-identifying information other dialing tones generated by a sender that are used to signal the recipient's customer premises equipment.").

3. NYPD also respectfully disagrees with Bell Atlantic's contention that information is *prima facie* not reasonably available if a carrier has to modify its system to provide law enforcement access to that information.⁴ In fact, the statute provides that if information is not reasonably available, a carrier does not have to modify its system to make it available. But it is up to the FCC to determine in the first instance whether a feature is reasonably available. It is clear from Congress' discussion of law enforcement's need for information that Congress anticipated that carriers would be required to make some modifications. Specifically, Congress recognized that carriers would need to make certain modifications despite having no other prevailing business reason for doing so. Accordingly, CALEA includes a reimbursement mechanism designed to compensate carriers for the costs incurred in making certain crucial alterations to existing systems.⁵

4. If implemented according to the legislative intent, CALEA will allow law enforcement, upon receipt of a legally issued order, to obtain information generated by the calling activities of criminal suspects regardless of the telecommunications technology used and, even more importantly, regardless of the telecommunications carrier that provides the suspect with service. The level of sophistication displayed by criminals has grown tremendously in recent years, a fact recognized by the industry itself. For example, in describing the utility of telecommunications technology to criminals, a vice-president of AT&T stated that ". . . the one component that has done more than any other to insulate the kingpin from law enforcement intervention is the

⁴ Bell Atlantic at 11.

⁵ 47 U.S.C. §1008.

telephone. . ."6 and that "[c]ellular phones are rapidly becoming the lifeblood of the contemporary narcotics enterprise."7 The NYPD has frequently observed that criminals intentionally use telecommunications services that are known to be impediments to surveillance technology. Any CALEA solution implemented must stop this practice by ensuring that, pursuant to a court order, law enforcement can receive information from all carriers.

5. There has been an overwhelming erosion of law enforcement's ability to conduct lawfully authorized electronic surveillance. Congress itself recognized that specific services and features jeopardized the effectiveness of electronic surveillance. NYPD does not share the industry's definition of *status quo*. The industry's interpretation of *status quo* would impede law enforcement's efforts and would only make allowances for the capabilities available to law enforcement at some point in the distant past. Rather, NYPD believes that a CALEA-compliant solution is a forward-looking one that makes available to law enforcement capabilities which are commensurate with its legal authority to conduct electronic surveillance.

Punch List

6. NYPD believes that the current industry interim technical standard, J-STD-025, is deficient. This interim standard lacks capabilities that are essential to law enforcement's continued effective use of lawfully authorized electronic surveillance as an investigative tool. Lawfully authorized electronic surveillance is a key investigative method used by law enforcement. Without the requisite capability to conduct lawfully authorized electronic surveillance

⁶ The Communications Revolution: A Drug Trafficker's Dream. Roseanne DeMaria, Corporate Vice President, Risk Management, AT&T Wireless Services.

⁷ *Id.*

commensurate with statutory authority, law enforcement's mission of protecting the public and ensuring its safety will be greatly impeded.

Content of subject-initiated conference calls

7. Industry claims that the subject of surveillance must be present during the course of a conference call for a carrier to provide information to law enforcement. This is based on the incorrect assumption that court orders are always written to cover specific individuals. There are numerous types of court orders, however, which are tailored to enhance law enforcement's efforts, while not intruding on the privacy of individuals. Court orders are issued identifying the equipment, facilities and services of a particular subscriber by listing a directory number. It is important to remember that the subscriber may or may not be the focus of the investigation. Carriers have never had, and will not have, access to the type of information that would allow them to determine whether a surveillance target is present during a conference call. Any assumption on the part of a carrier that the subscriber and subject of investigation are one and the same is no more than an assumption.

8. Many of the comments received by the Commission⁸ argue that this capability is outside the scope of CALEA and that because law enforcement currently does not receive this information, the Commission should not include the capability in its final rule. NYPD strongly disagrees. The legislative history clearly and specifically identifies conference calling⁹ as one example of the features and services CALEA is intended to include. The fact that law enforcement does not currently receive this information should be considered by the Commission

⁸ See, e.g., Ameritech at 6; Bell Atlantic at 4; SBC at 12; PCIA at 22.

⁹ H. Rep. 103-827, 103d Congress, 2d Sess at 9 (1994) ("H.Rep.")

as one of the driving forces behind Congress' passage of this vital legislation.

9. Other comments refer to the conditional nature of this capability and the absence of carrier liability in the event that law enforcement does not request the provision of adequate delivery facilities.¹⁰ NYPD agrees with AT&T ". . . that this capability is conditional and subject to adequate provisioning to monitor all active surveillance."¹¹ Furthermore, NYPD expects that during the course of its continued interaction with telecommunications carriers, those carriers will notify NYPD of the number of channels which should be provisioned based on the features and services to which a subject of lawfully authorized electronic surveillance subscribes. It is interesting to note that both AT&T and CTIA are simultaneously arguing that this capability is not required by CALEA, yet are prepared to outline the conditions of delivering this information to law enforcement.

10. With respect to carriers' responsibility to provide the content of conference calls, NYPD agrees with the Commission and many of the submitted comments that it is necessary for the equipment, facilities or services identified on the lawful authorization to be in use for law enforcement to receive this information. If the equipment, facilities or services identified on the lawful authorization are no longer in use, law enforcement will be denied this information.

11. Subscribed-to conference calling is a service that many criminals use to circumvent law enforcement efforts to conduct lawfully authorized electronic surveillance. In fact, during the

¹⁰ AT&T at 7; CTIA at 24.

¹¹ AT&T at 7.

deliberative process leading to the passage of CALEA, Congress recognized conference calling as an impediment to law enforcement. Conference calling places a restriction on law enforcement's ability to conduct effective surveillance because the subject of surveillance, the subscriber or someone else, can make use of the service from anywhere. In other words, the subject of surveillance can be on the conference leg that is associated with the directory number, or any of the other legs of a conference call.

12. In the case of a conference calling service in which service is pre-subscribed, there is an association between a directory number, and the equipment, facilities and services that anyone may use by accessing the network through that directory number. It is of no consequence whether a particular person is using the handset associated with the directory number, or any other leg of a conference call. In many cases, the subject of surveillance knows enough about how carriers provide conference calling to make use of his conference calling service by acting as one of the conference legs, and not the primary handset associated with the directory number. During the course of a conference call, the carrier has no way of determining which leg of the conference call the subject of surveillance is using for two reasons. First, as mentioned above, the carrier has no way of know the subject of surveillance. Second, the subscriber can be on any of the legs of a conference call.

13. Many carriers maintain that it is their responsibility to protect the privacy of individuals not subject to surveillance during the course of a conference call. It is NYPD's position that, during the course of a conference call, the carrier has no way of determining which leg of the conference call the subject of surveillance is using, or even knowing which party is the subject of

surveillance. Furthermore, law enforcement is required by law to minimize the information it receives when that information is not germane to the criminal activity under investigation.

14. Another type of conference calling capability, known as "meet-me" conference, was also the subject of some comments.¹² It is NYPD's position that carriers providing "meet-me" conference call services are subject to both lawfully authorized electronic surveillance and the requirements of CALEA. For law enforcement to obtain lawful authorization to conduct electronic surveillance on a "meet-me" conference call, it must have previous knowledge of the conference call. NYPD does not expect any carrier to provide it with the ability to conduct lawfully authorized electronic surveillance of features or services to which a subject of surveillance does not subscribe.

Party Hold, Party Join, Party Drop

15. Law enforcement's need for information generated under this capability for evidentiary justification purposes cannot be understated. There is an absolute necessity for law enforcement to have the ability to identify when particular portions of a call are active, placed on hold, joined back into a call, or dropped from a call entirely. While comments submitted to the Commission characterize this capability as "costly and complex,"¹³ it is the position of the NYPD that prior to the introduction of services allowing individual subscribers to control the nature of communications, law enforcement had access to the participating directory numbers of any

¹² See, e.g., AT&T at 7; Bell South at 15; CTIA at 24.

¹³ Airtouch at ii.

telephone call.

16. It is important to point out a significant difference between law enforcement's ability to monitor participants during the course of a call in the wireline network versus a wireless network.

In a wireline environment, a subscriber must use the flash hook to control the status of a call. That flash hook is recognized by law enforcement equipment today. In a wireless environment, that is not the case. Nextel states ". . . the party message information [is] not available today at all . . ." ¹⁴ NYPD believes it important for the Commission to know a wireless carrier serving the New York area currently has the capability to provide party hold and drop messages today using equipment that is already in place. This capability is provided because carriers and manufacturers were responsive when law enforcement expressed its evidentiary needs for this capability. NYPD is concerned that if this capability is not expressly identified in the Commission's final rule, other carriers and manufacturers will not accept the responsibility of providing this capability to law enforcement.

17. Other comments claim that "whether a party joins or drops from a call has no bearing on the continuity of a call or the communications that may be made during the call." ¹⁵ NYPD disagrees with the implication that this information is unimportant to law enforcement. NYPD is most troubled by the comments of Bell Atlantic. Bell Atlantic contends that "conference call capabilities are often provided through equipment that is external to the switch...[and] [t]his equipment 'knows' what calls are part [of] a particular conference and when parties are added to

¹⁴ Nextel at 9-10.

¹⁵ AT&T at 9.

or dropped from a conference, while the switch does not."¹⁶ Bell Atlantic makes the assumption that only switches will or should be involved in electronic surveillance. While law enforcement can not dictate solutions, NYPD believes that limiting solutions to switches unfairly restricts law enforcement's fundamental authority to conduct electronic surveillance. Finally, NYPD believes that each and every carrier records when participants drop from calls for billing purposes.

Subject-initiated dialing and signaling

18. NYPD offers the following forthright examination of subject-initiated dialing and signaling information available to law enforcement at one point in time. The example is call forwarding service. When call forwarding was initially introduced into the network, law enforcement received information pertinent to the forwarded-to number. That success was in large part due to the fact that law enforcement had access to information passed between the subject of surveillance and the network. The introduction of call forwarding did not change this because when a subscriber initiated the call forwarding feature associated with the directory number under surveillance, the call forwarding feature was activated and changed from the physical device associated with the directory number. Any change to the forwarded-to number necessarily came from the same device and was available to law enforcement.

19. With the introduction of remote activation of call forwarding, that ability disappeared. Today, law enforcement has no way of knowing where calls will terminate. Bell Atlantic states that the current industry interim standard "would not, quite correctly, require the carrier to inform law enforcement that the surveillance subject has invoked or deactivated the call forwarding

¹⁶ Bell Atlantic at 11-12.

feature."¹⁷ NYPD reiterates its agreement with the Commission's tentative conclusion that this capability is no more than the retention of the status quo.

In-Band and Out-of-Band Signaling

20. Airtouch claims that "[a] cellular system generates out-of-band signaling messages constantly, including supervisory audio tones, control channel messages, and other signals..."¹⁸

Carriers would have the Commission believe that law enforcement is seeking a broad, expansive (perhaps even exhaustive) list of messages. To the contrary, law enforcement seeks a very limited number of messages. During the consultative process leading to the industry's adoption of the interim standard, law enforcement indicated that it was focusing on those signals that are humanly perceivable. This concept is reflected in the wording of the current Enhanced Surveillance services (ESS) ad-hoc working group,¹⁹ as well as in the final rule: messages that the network intends the subject to see (display or lamps), hear (cause tones to be generated), or feel (vibration in lieu of tones). Airtouch's comments about messages as audio tones is confusing. In analog cellular systems, there are tones around 6 kHz that let the handset know that it is locked onto the correct radio channel which are not intended to be heard by the user, and thus, are usually muted. Law enforcement does not seek access to this particular type of message.

21. Airtouch also comments that ". . . a pen register would not have identified the effects of the transmission of those tones resulting from the party's activation or deactivation of call

¹⁷ Bell Atlantic at 9.

¹⁸ Airtouch at 20.

¹⁹ After the industry's adoption of its interim standard, the industry formed the Enhanced Surveillance services (ESS) ad-hoc working group to address those capabilities identified by law enforcement as missing from the interim standard. Efforts to standardize those capabilities have proceeded since the ad-hoc's group inception in early 1998.

forwarding."²⁰ Under the *status quo* for in-band and out-of-band signaling, law enforcement receives signals such as ringing, busy signals, and flash hooks. NYPD suggests that because carriers do not actively participate in evidence collection or in obtaining corresponding legal authority, carriers are not best suited to determine what information can be gleaned by law enforcement during the course of an investigation. As mentioned previously, NYPD disagrees with the position of Airtouch. When it was introduced, call forwarding could be activated only from the physical handset to which the service was provided. Additionally, star tones (*72, *73) were a dead giveaway that call forwarding was being changed, activated or deactivated.

22. NYPD agrees with the Commission's tentative conclusion that call forwarding information is considered call-identifying information. The NYPD has numerous real-life examples, many of which pertain to narcotics investigations, in which this capability has proven vital. The importance of knowing where the subject of surveillance is expecting to receive calls before those calls are placed cannot be underestimated. This information identifies the termination (or expected termination) of incoming calls. Again, NYPD stresses the investigative importance of this capability. This information was formerly available to law enforcement. With particular respect to signals such as ringing, NYPD's extensive experience investigating the criminal element shows that they are adept at using signals (e.g., two rings of a telephone) to communicate.

²⁰ Airtouch at 17.

23. Today, with the use of a filter at the telephone pole that passes everything except audio, a dialed number recorder detects tones such as those used in call waiting. By not including this capability, law enforcement would receive *less* than the *status quo*. Ameritech states that ". . . the FBI seeks information on the status of a non-completed call, i.e., whether the called line was busy or merely rang with no answer."²¹ In the case of wireline electronic surveillance, NYPD and all of law enforcement receive this information today.

24. Bell Atlantic states that ". . . the notification sent by a voice mail service . . . is the entire content of the communication, not information to identify the call." The NYPD cannot imagine any circumstances in which this can be viewed as call content. In this instance, the content of the communications is the voice mail message that is left with the voice mail service. Furthermore, message waiting indicators such as stutter dial tone are available using traditional electronic surveillance techniques.

Timing

25. Comments submitted addressing the Commission's tentative conclusions regarding timing range from assertions that the current industry interim standard is sufficient;²² to contentions that carriers do not provide this capability today, and, therefore, should not provide this information in the future;²³ to claims that timing should not be considered by the Commission as call-identifying information.²⁴ NYPD disagrees with these arguments. The ability to correlate call data and call

²¹ Ameritech at 8.

²² Ameritech at 10.

²³ Bell Atlantic at 3.

²⁴ AT&T at 15.

content is essential to meet law enforcement's obvious evidentiary needs.

26. The Commission should disregard Airtouch's comment that ". . . time-stamp proposal would effectively require that wireless carriers redesign [their networks]"²⁵ in light of the NYPD's current experience with service providers in the New York area on the issue of timing. Some carriers have deployed wireless systems that delivery call content and call data to law enforcement separately. The manufacturers of this equipment have been able to meet law enforcement's critical evidentiary need by delivering call data associated with call content within one second. This is today's standard method of operation for electronic surveillance.

27. NYPD notes that AT&T ". . . can understand and even support a requirement for timing requirements in the standard . . ." ²⁶ NYPD disagrees, however, with AT&T's recommendation that ". . . the timing requirement for delivery should be expressed as a percentage so that delivery occurs within the timing requirement at least 95% of the time."²⁷ NYPD has consistently maintained that the services made available to law enforcement should be no less reliable than regular subscription service. The 95% requirement stated in AT&T's comments is far below the standard of service currently provided to subscribers.

Surveillance status, continuity check tone, feature status

²⁵ Airtouch at 21.

²⁶ AT&T at 14.

²⁷ AT&T at 15.

28. It is noteworthy that CALEA brings about a paradigm shift to the fundamentals of electronic surveillance. CALEA necessitates that carriers take a larger part of the mechanics of electronic surveillance. Because of the sophistication of the telecommunications network, and the corresponding sophistication of any electronic surveillance solution, carriers will be in control of electronic surveillance. CALEA recognized that law enforcement can no longer be effective on the fringe of the telecommunications network. These three capabilities (surveillance status message, continuity check tone, feature status message) represent *one* uniform way for the telecommunications industry to meet its obligation to *ensure* the integrity of electronic surveillance. Despite commenters' concurrence with the Commission that these capabilities are not required by CALEA, NYPD maintains that they are extremely necessary. Previously, access to the local loop was adequate because the network was relatively simple, and the subscriber had little ability to manipulate the services and features to which he subscribed. As network intelligence has expanded outwardly to the subscriber, law enforcement has lost a significant portion of its ability to conduct effective electronic surveillance.

29. The surveillance status message is one way for carriers to ensure law enforcement that lawfully authorized electronic surveillance has been activated by carriers on the correct equipment, facility or service. By informing law enforcement of the directory number on which electronic surveillance has been activated, carriers will facilitate the protection of the privacy of communications not authorized to be intercepted. As mentioned in NYPD's comments, in some instances where carriers activate electronic surveillance they have activated surveillance on the wrong subscriber.

30. NYPD disagrees with AT&T's comment that ". . . the 'ensure' language imposes an obligation on carriers and manufacturers to design future equipment, facilities and services to support wiretaps."²⁸ This overall obligation of carriers and manufacturers is the central tenet of CALEA, and does not stem from one particular phrase. Every carrier is obligated to ensure that its equipment, facilities, or services can meet the individual assistance capability requirements of section 103 of CALEA.²⁹

31. Carriers' provision of a continuity check tone is analogous to carriers' provision of dial tone on any subscriber's line. Today dial tone is provided on every subscriber's line for two reasons: (1) to alert the subscriber that the switch is ready to accept dialed digits; and (2) to alert the subscriber that the facilities connecting telephone to network are in working order. Under the *status quo* for lawfully authorized electronic surveillance, law enforcement knows the facilities are in working order. NYPD agrees with the comments of SBC ". . . that a simple continuity check tone on call content channels could be employed to notify law enforcement when a surveillance is active."³⁰ Furthermore, NYPD agrees with SBC in its assertion that "[t]his method would avoid the need for human intervention to periodically check the circuit manually."³¹

32. As telecommunications technology continues to outpace rapidly law enforcement's ability to conduct lawfully authorized electronic surveillance, the feature status message becomes more and more vital. Subscribers will no doubt be able to configure and re-configure future services

²⁸ AT&T at 15.

²⁹ 47 U.S.C. §1002(a).

³⁰ SBC at 16.

³¹ SBC at 17.

and features. For example, the industry interim standard imposes a restriction on a law enforcement with respect to call forwarding. As described previously, the ability of a subscriber to change the number to which incoming calls are forwarded from any location has had a devastating effect on criminal investigations. NYPD disagrees with the Commission and commenters³² that this information is not call-identifying information. NYPD firmly believes that the destination of any call should be considered call-identifying information. Most importantly, prior to the introduction of remote activation of call-forwarding, law enforcement had the ability to collect this call-identifying information and, thus, it is essential in order to maintain the *status quo*.

Dialed digit extraction

33. NYPD believes that the discussion of dialed digit extraction is an example of the fundamental misinterpretation of the division of responsibilities under CALEA and under other applicable electronic surveillance statutes. CALEA was written to clarify the telecommunications industry's technical responsibility to design and develop solutions which would apply to equipment, facilities or services. When law enforcement obtains lawful authorization to conduct electronic surveillance, it obtains lawful authorization to gain access to specific equipment, facilities or services. When specific equipment, facilities or services are identified on a court order, by directory number or otherwise, law enforcement necessarily expects access to all call-identifying information and/or the content of communications supported by the equipment, facility or service.

³² See, e.g., Nextel at 17; PCIA at 22.

34. NYPD currently receives post-cut-through dialed digits when it conducts lawfully authorized electronic surveillance on subscribers of wireline services. This is accomplished by simply placing a bandpass, or audio filter at the intercept access point (IAP), which is the physical interception point on the local loop. But even more importantly, some of today's advanced wireless systems have the capability to provide this information on a separate data channel, as described in the punch list. NYPD fears that if this capability is not recognized as a requirement of CALEA, there will be a *de facto* repeal of the information currently obtained because carriers would be free to stop providing this information. This information is a vital investigative tool and is the only realistic way for law enforcement to determine the final destination of some calls made by a target of lawfully authorized electronic surveillance.

35. Some carriers mistakenly ascribe the responsibility to minimize access to call content to themselves, rather than to the law enforcement agency that lawfully obtains the right to install a pen register.³³ Other members of the industry have shown a lack of understanding with respect to the way law enforcement adheres to *its* requirement³⁴ to minimize information gained through lawfully authorized electronic surveillance that does not pertain to the criminal investigation at hand.³⁵ In fact, in the normal course of criminal investigations involving electronic surveillance, law enforcement spends more time *not* listening because most conversations are not germane to the case. Although carriers assume it is their responsibility to minimize intrusion on subscribers' privacy, the judicial system is the appropriate place for balancing law enforcement's need for

³³ See, e.g., Nextel at 20.

³⁴ 18 U.S.C. §3121(c).

³⁵ See, e.g., SBC comments at 17-18.

information with privacy rights.³⁶

36. Some carriers contend that, from the perspective of a local exchange carrier, a call is terminated at the inter-exchange carrier's platform.³⁷ They propose that law enforcement obtain dialed digit extraction information from long distance carriers.³⁸ The NYPD would like to point out, however, that the Commission has recognized that a call is "completed" when the called party answers the call, not when it is connected to an 800 calling card service.³⁹ Thus, local exchange carriers should be required to provide law enforcement with post-cut-through digits. Moreover, placing this responsibility with long distance carriers would require law enforcement to contact *every* long distance carrier because subscribers are able to change long distance carriers on a per call basis. This solution is also implausible because subscribers can use calling cards and inter-exchange equal access to place long distance calls. It would be impossible for law enforcement to conduct effective pen registers under these circumstances. In an effort to attain overall cost-effectiveness, the Commission should affirm its tentative conclusion.

37. AT&T comments on dialed digit extraction and the cost of a typical decoder. In response,

³⁶ See, e.g., Airtouch at 8; Ameritech at 12.

³⁷ See, e.g., US West at 19.

³⁸ Bell Atlantic at 9.

³⁹ See Implementation of the Pay Telephone Reclassification and Compensation Provisions of the Telecommunications Act of 1996, Report and Order, CC Docket No. 96-388 (1996) at 32-33.

the NYPD believes that carriers could pool decoders, like they currently do, but for longer periods of time in order to capture post-cut-through dialed digits. Carriers are in the best position to determine, through traditional telephone traffic engineering techniques, the most cost effective method of supplying these resources.

38. The United States Supreme Court⁴⁰ and the New York Court of Appeals⁴¹ have held that subscribers have no expectation of privacy to the numbers dialed because they are always provided to the subscriber's telecommunications carrier. CALEA mandates that law enforcement has the responsibility to sort out numbers that are not part of call-identifying information, unless the carrier has the technical means to do so.

Reasonably available

39. Many commenters state that the industry interim standard ". . .gets the definition of reasonably available just right. . ."42 Nextel goes on to state that ". . .the distinction between call billing records and pen registers is disappearing and Nextel understands that law enforcement regularly demands and is satisfied with billing records as they are generated in lieu of pen register

⁴⁰ See Smith v. Maryland, 442 US 735.

⁴¹ See New York v. Bialostok, 80 N.Y.2d 738 (1993).

⁴² See, e.g., Nextel at 5

data."⁴³ The options presented to NYPD by Nextel are to either accept billing records or receive no information at all. Given that choice, NYPD accepts billing records. As mentioned previously, NYPD believes that a CALEA-compliant solution is one that makes available to law enforcement capabilities which are commensurate with its legal authority to conduct electronic surveillance.

Extension of the June 30, 2000 deadline for J-STD-025

40. The CALEA implementation process must not be delayed. Public safety cannot be further compromised or frustrated. Congress recognized in the early 1990's that law enforcement's ability to conduct electronic surveillance was slipping away, and reacted by passing CALEA. The safety of Americans must not be jeopardized by further delaying the implementation of this legislation.

41. The Commission established a separate deadline for the industry's compliance with the capabilities found to be required by CALEA. But Congress envisioned that there would be solutions already available and its original intent to protect the public should have long been realized. The industry has argued, and will no doubt continue to argue, that additional delays are necessary so that it can contemplate the most effective way to incorporate these capabilities into a standard. The Commission should weigh this argument with the industry's overall intention to lessen its responsibilities under the Act, and its attempts to delay the process for as long as possible.

⁴³ Nextel at 5

42. Industry claims that the punch list has not been articulated with sufficient precision.⁴⁴ The NYPD contends that the industry's complaints about the punch list's alleged lack of clarity is no more than a delay tactic. The NYPD was present during years of standards meetings and can assure the Commission that industry's arguments are invalid. Manufacturers of telecommunications equipment were present in meetings during the years leading to the industry interim standard and have had the opportunity to seek exhaustive clarification from law enforcement. In fact, many of those manufacturers have made significant progress in meeting CALEA's requirements by providing features such as post-cut-through dialed digits.

43. Technical questions raised by the industry were examined and answered. Technical contributions were submitted to every request made by the standards group. In fact, there were many times where law enforcement instigated this process. Sadly, in the current process within TR45.2, and the ad-hoc working group known as the ESS (Enhanced Surveillance Services), the industry has currently suspended activity, not due to the lack of law enforcement participation, but rather as a result of industry apathy.

44. Industry also alleges that the punch list came *after* J-STD-025 emerged from the process of standardizing capabilities.⁴⁵ To the contrary, all the capabilities identified by law enforcement as essential evidentiary and minimization requirements were in a draft version of the industry standard at one time. The industry would have the Commission believe that these capabilities were *added* to an already developed standard, as an additional layer of capability that law enforcement considered supplemental to the J-STD-025. In fact, these capabilities were

⁴⁴ Airtouch at 2.

⁴⁵ Airtouch at 5.

components of law enforcement's consideration of electronic surveillance requirements. They are central to law enforcement's ability to conduct effective electronic surveillance.

45. The industry has devoted the efforts of an entire ad hoc working group for over a year to develop standards for the missing capabilities, yet the industry claims that it does not possess the understanding of the punch list in sufficient detail in order to provide manufacturers with a standard. The NYPD notes that Congress intended to hold the industry responsible for Section 103⁴⁶ capabilities even in the absence of a standard.

Commission's role in the remand of the standard

46. NYPD supports CTIA's suggestion that the Commission attend every standard meeting associated with the punch list.⁴⁷ The NYPD submits that the Commission should witness the injustice and arrogance perpetuated by this industry, and its total disregard for public safety.

The need to modify systems

47. Industry claims that Congress never intended that any of its systems must be modified for the sole purpose of making call-identifying information available.⁴⁸ The NYPD believes that if information is available within a carrier's network or system(s) for some other purpose, it is inherently available. Law enforcement is not arguing that new information needs to be created. Rather, existing information should be made available to law enforcement pursuant to lawful authorization. Even the J-STD-025, in its present deficient form, requires some level of modification. Taken to the extreme, this position would mean CALEA could never be

⁴⁶ 47 U.S.C. §1002.

⁴⁷ CTIA at 37.

⁴⁸ *See, e.g.*, PCIA at 32; Bell Atlantic at 11; Bell South at 11.

implemented because, as the industry sees it, no change, however insignificant, is required under the guise of reasonably available.

Repeated characterization of this issue as an FBI or DOJ issue.

48. A number of commenters portray the FBI and DOJ as the only law enforcement agencies affected by the CALEA implementation effort. This characterization ignores the many hundreds of police departments across the country that rely on lawfully authorized electronic surveillance to investigate and prevent criminal activity. NYPD urges the Commission to disregard all industry attempts to mischaracterize the role of all law enforcement agencies and to diminish the importance of electronic surveillance to public safety.

ESI Simulator

49. NYPD and other law enforcement agencies were consulted on issues pertaining to the ESI Simulator and were involved in the various stages of its development. As an active participant in the standards process, and as the nation's largest police force, NYPD can attest to the accuracy of the simulation capability. The messages and information depicted by the ESI Simulator are an accurate representation of the current industry standard and its deficiencies.

Cost

50. NYPD is subject to non-disclosure agreements, at the request of the industry. However, NYPD feels strongly that cost should not be a deciding factor in determining what capabilities are necessary to protect public safety. In Section 109 of CALEA,⁴⁹ Congress provided thoughtful, extensive safeguards to ensure that carriers are not overly burdened by the cost of implementation.

51. In the early days of cellular telecommunications, NYPD voiced concern to carriers that its ability to conduct lawfully authorized electronic surveillance was being significantly hampered. The industry responded by developing certain capabilities for law enforcement. Based on NYPD's experience, the cost of CALEA-compliant electronic surveillance solutions may be significantly less than the gross estimates of carriers. NYPD has attached information regarding the deployment of the electronic surveillance solution currently in use by Bell Atlantic in the New York Metropolitan region. While this solution should not be considered CALEA-compliant, it affords the Commission the opportunity to learn about how carriers have recovered the cost associated with current capabilities. Further, it highlights the existing relationship between law enforcement and telecommunications carriers and the willingness of both parties to share in the costs associated with electronic surveillance. In the cost reimbursement model referred to in the attachment, a carrier invested the capital to make electronic surveillance capabilities available to law enforcement and then recouped its costs over time by charging law enforcement a fee for service. Once the initial costs of development and deployment had been recovered, the fee for service was rescinded.⁵⁰

52. The Commission should also consider the cost that the telecommunications industry currently levies against law enforcement to conduct electronic surveillance. These rates are

⁴⁹ 47 U.S.C. §1008.

⁵⁰ It must be noted that the solution developed as a result of this agreement has technical deficiencies and was deployed prior to the passage of CALEA, but can be considered a benchmark for the order of magnitude of the costs associated with CALEA.

considerable. The following is a representative sample of the rates charged to NYPD for "assistance": \$250 per month, per switch for a pen register; \$450 per month for Title III; \$150 per month, per box for voicemail. The figures do not include the necessary leased lines to deliver the information to law enforcement. The Commission should consider how these rates compare with rates charged to regular subscribers. NYPD believes that carriers are currently recovering a significant portion of their capital expense through the fees they charge law enforcement.

FCC role in future standard decisions

53. Because there is irrefutable evidence that the criminal element relies heavily on advanced telecommunications services, the NYPD believes that the Commission will be called upon to resolve many future discrepancies between the industry and law enforcement.

Law enforcement dictating a specific design

54. Many commenters contend that law enforcement is dictating a design by advocating the inclusion of some or all of the capabilities that are missing from the interim standard.⁵¹ The nine missing capabilities are central to law enforcement's ability to conduct effective lawfully-authorized electronic surveillance. The NYPD is not concerned with the method by which a manufacturer or carrier provides the information; the NYPD's only concern is that the information

is provided in a consistent and reliable manner.

⁵¹ Airtouch at 1.

Conclusion

55. NYPD, and law enforcement in general, is the customer requesting a particular service from the telecommunications industry. Based on NYPD's understanding of the electronic surveillance statutes it operates under everyday, the industry interim standard is deficient. The Commission's tentative conclusions to include five of the nine missing capabilities (content of conference calls; party hold, party join, party drop messages; subject initiated dialing and signaling; timing; and dialed digit extraction) go a long way in resolving that discrepancy. However, the remaining four capabilities (in-band and out-of-band signaling; surveillance status message; continuity check tone; and feature status message) are critical to ensure law enforcement's ability to conduct effective and lawful electronic surveillance.

DATE: January 27, 1998

Respectfully submitted,

John Pignataro
Sergeant Detective Supervisor
Electronic Surveillance Technical Advisor
New York City Police Department

Edward T. Norris
Deputy Commissioner, Operations
New York City Police Department

Attachment

NYNEX Mobile Communications Company
2000 Corporate Drive Orangeburg NY 10962 2024
1 800 227 1089

NYNEX
Mobile Communications 

July 13, 1992

New York Police Department
1 Police Plaza
Room 1200P
New York, NY 10038
Attn: John Pignataro

Dear Mr. Pignataro:

On May 20, 1992, NYNEX Mobile held a meeting with a number of law enforcement agencies to discuss the technical aspects and costs of providing two new software packages that are now available.

The first of the two, Increased Court Order Surveillance, (ICOS), provides the software equivalence of twenty-four trap circuit ports that are utilized with NMC equipment. With ICOS, NYNEX Mobile now has available to law enforcement the functional equivalence of a total of thirty-one ports. (The ICOS system ultimately can be expanded to ninety-six ports). The cost paid by NMC for ICOS software and related hardware (interfaces) was \$257,203.00. Attendees at the May 20, 1992 meeting agreed that each mobile number activated on ICOS will be charged \$500.00 for a thirty day period. (Mobiles that have been activated for fourteen days or less will be charged \$250.00.) NYNEX Mobile will continue to bill for ICOS until the total cost of the system has been recovered. The software and equipment cost recovery charges will then cease.

The second system NYNEX Mobile has made available is the Surveillance/Monitoring and Reporting/Tracking (SMART) System. SMART provides calling activity details that can be accessed by telephone from any location with a computer terminal and modem.



NYNEX Recycles

- 2 -

At this time, up to five modems can access SMART simultaneously. Attendees agreed that SMART should not be logged onto for any great length of time, so as to permit other agencies to access it as needed. The cost of the SMART System software totaled \$37,543.75. NYNEX Mobile will bill \$200.00 a month for each mobile number activated on the SMART System. (\$75.00 will be charged for mobile numbers that have been activated for one to eight days.) Billing for SMART software cost recovery will end once these charges have been recovered.

Very truly yours,

Patricia Grimaldi
Patricia Grimaldi
Supervisor Security Specialists

PG/rr