

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)	
)	ET Dkt. 04-295
Communications Assistance for Law)	RM-10865
Enforcement Act and Broadband Access and)	
Services)	

**COMMENTS OF THE
NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION**

Of Counsel:
Christopher W. Savage
Cole, Raywid & Braverman, LLP
1919 Pennsylvania Avenue, N.W.
Suite 200
Washington, D.C. 20006
(202) 659-9750

November 8, 2004

Daniel L. Brenner
Neal M. Goldberg
Michael S. Schooler

National Cable & Telecommunications
Association
1724 Massachusetts Avenue, N.W.
Washington, D.C. 20036
(202) 775-3664

INTRODUCTION AND SUMMARY	2
I. THE CABLE INDUSTRY HAS BEEN RECOGNIZED BY LEAs AS A KEY SUPPORTER OF EFFORTS TO CONDUCT LAWFUL SURVEILLANCE IN CONNECTION WITH NEW TECHNOLOGY.....	2
A. The Cable Industry Has Provided a Technical Solution for Applying CALEA to Cable’s VoIP Service.....	2
B. The Cable Industry Supports the Applicability of CALEA to VoIP Services as a Matter of Law.....	5
C. Applying CALEA to Broadband Internet Access Services Raises Technical Issues Distinct From Those Affecting VoIP.....	7
II. CABLE CAN PROVIDE A NUMBER OF THE CAPABILITIES DISCUSSED IN PARAGRAPH 66 OF THE <i>NPRM</i>	8
A. Cable Can Deliver Certain Information About Subjects’ Access Sessions.....	10
B. Cable Can Provide Information about a Subject’s Service and Account Profiles.....	10
C. Cable Can Provide Law Enforcement Agencies Information About Packets Sent and Received by the Subject.....	11
III. ADDITIONAL GUIDANCE IS REQUIRED ON CERTAIN MATTERS DISCUSSED IN THE <i>NPRM</i>	12
A. Clarification of the Definition of “Access Session” in the Broadband Context Will be Required to Develop a Workable Surveillance Specification.	13
B. Both Service Providers and Law Enforcement May Face Bandwidth Constraints Due to the Huge Amounts of Data Potentially Subject to Surveillance.	14
C. A Reasonable Compliance Period Will be Required.....	15
IV. CABLELABS QUALIFIES AS AN "INDUSTRY ASSOCIATION OR STANDARD-SETTING ORGANIZATION" UNDER CALEA SECTION 107(a)(2).	16
CONCLUSION.....	19

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)	
)	ET Dkt. 04-295
Communications Assistance for Law)	RM-10865
Enforcement Act and Broadband Access and)	
Services)	

**COMMENTS OF THE
NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION**

The National Cable & Telecommunications Association (“NCTA”) hereby respectfully responds to the *Notice of Proposed Rulemaking* (“NPRM”) in the above-captioned matter.¹

NCTA is the principal trade association of the cable television industry in the United States.

NCTA’s members include the operators of cable television systems serving more than 90 percent of the nation’s cable subscribers. They also include more than 200 cable program networks, as well as companies that provide equipment and services to the industry. NCTA’s members are leaders in the deployment of Broadband Internet Access services (*i.e.*, cable modem service) and are in the forefront of those deploying Broadband Telephony (*i.e.*, VoIP services). As discussed below, the cable industry has also been a leader in working with law enforcement agencies in accommodating legitimate law enforcement needs to new technology deployment.

As described below, the cable industry continues to support the efforts of law enforcement agencies (“LEAs”) efforts to apply the Communications Assistance for Law Enforcement Act (“CALEA”) to new technologies.

¹ In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services, ET Docket No. 04-295, RM-10865, *Notice of Proposed Rulemaking and Declaratory Ruling*, FCC 04-187, released August 8, 2004 (“NPRM”).

INTRODUCTION AND SUMMARY

In the *NPRM*, the Commission addresses a myriad of questions surrounding the legal, technical and practical issues that arise in attempting to apply the provisions of CALEA to Voice over Internet Protocol (“VoIP”) services as well as “Broadband Internet Access” services, such as cable modem service. In these comments, the cable industry continues its role as a leader in working with the Commission and LEAs by supporting the LEAs’ goals in this proceeding.

In particular, we reiterate that:

- Cable’s VoIP services may be subjected to CALEA as a legal matter without implicating the regulatory classification of those services for Communications Act purposes;
- As the FBI has recognized, the CableLabs’ PacketCable™ Electronic Surveillance Specification provides the means for compliance with CALEA for cable’s VoIP services;
- Regardless of the ultimate holding on the applicability of CALEA to cable modem and other Broadband Internet Access services, the cable industry stands ready to work with LEAs to meet their legitimate surveillance needs if additional guidance on issues raised in the *NPRM* is provided; and
- Given the plain words of the statute and LEA recognition of CableLabs’ key role in developing the PacketCable™ Electronic Surveillance Specification, the Commission should conclude that CableLabs qualifies as an “Industry Association or Standards Setting Organization” under Section 107(b) of CALEA.

I. THE CABLE INDUSTRY HAS BEEN RECOGNIZED BY LEAs AS A KEY SUPPORTER OF EFFORTS TO CONDUCT LAWFUL SURVEILLANCE IN CONNECTION WITH NEW TECHNOLOGY.

A. The Cable Industry Has Provided a Technical Solution for Applying CALEA to Cable’s VoIP Service.

The cable industry has led the way in the deployment of residential broadband technology throughout the country. And, while the legal landscape surrounding CALEA applicability to such technology has not been clear, the cable industry has nevertheless been at the forefront of

meeting the technical challenges LEAs face to implement CALEA's lawful surveillance assistance obligations as applied, in particular, to Voice over Internet Protocol services.

Even though CALEA's applicability to VoIP was not settled, the cable industry concluded that the responsible course was to ensure that cable systems deploying a VoIP capability would be in a technical position to be able to comply with CALEA. As a result of this approach, CableLabs, the cable industry's technical arm, adopted its first lawful surveillance specification for voice communications over cable systems at the end of 1999 – nearly five years ago. In the intervening years, the cable industry has worked with equipment vendors and others – including, specifically, representatives of law enforcement – to refine and improve its PacketCable™ lawful surveillance specification.

The most recent version of this specification was issued in July 2004 and fully accommodates all of the needs of LEAs that have been articulated to the cable industry. As Richard Green, CableLabs' President and CEO, recently testified:

The cable industry has met all of the FBI's needs with regard to VoIP. Specifically, CableLabs succeeded by July 2004 in resolving *every* issue on the FBI's "wish list" for CALEA compliance by cable's VoIP services, including:

- Subject-initiated conference calls – provides law enforcement with the content of subject-initiated conference calls.
- Timing Information – allows law enforcement to correlate call identifying information with call content.
- Subject-initiated dialing and signaling – provides law enforcement with access to all subject dialing and signaling information such as use of flash hook (call waiting) and feature keys.
- In band/out-of-band signaling – notifies law enforcement whenever subject's service sends a tone or other network message such as if a line is ringing or busy.
- Party Hold/join/Drop – allows law enforcement to identify the active parties to a subject-initiated call.
- Dialed Digit Extraction – provides law enforcement those digits dialed by a subject during a call.

Testing of cable equipment built to these specifications will begin in February 2005, and products that do not meet the latest version of the PacketCable Electronic Surveillance Specification will not be CableLabs' certified – nor are they likely to be purchased by cable operators.²

The FBI's response to the issuance of this specification was very positive, as is evidenced by the following excerpt from a recent FBI Press Release:

“The latest issue of this technical specification represents a milestone in the cable industry's efforts to address law enforcement's concerns regarding VoIP (Voice over Internet Protocol) services made available by cable companies,” stated Kerry Haynes, FBI Assistant Director responsible for Investigative Technologies.

Mr. Haynes added: “This specification is an extremely positive development which ultimately will empower federal, state and local law enforcement agencies with the technical capability to continue to protect the public by effectuating court-authorized electronic surveillance.

We look forward to working with the industry in its development of technical solutions based on this specification and with companies as they implement solutions into their IP networks.”

In summarizing the recent cable specification, Assistant Director Haynes stated “this document is an extraordinary example of law enforcement and industry collaboration in the public interest. It stands as a model for future industry-law enforcement cooperative efforts.” Mr. Haynes extended special recognition and appreciation to Time-Warner, Comcast, Cablevision, and Cox for their diligent efforts in collaboration with CableLabs to achieve this milestone in the provision of critical electronic surveillance capabilities to law enforcement.”³

² Testimony of Richard R. Green, President and Chief Executive Officer, Cable Television Laboratories, Inc., on Law Enforcement Access to Communication Systems in the Digital Age, before the Subcommittee on Telecommunications and the Internet, Committee on Energy and Commerce, U.S. House of Representatives, September 8, 2004, at 4-5.

³ *Federal Bureau of Investigation Calls CableLabs' Release of its PacketCable™ Electronic Surveillance Technical Specification “A Positive Development” for Cable Industry Compliance with the Communications Assistance for Law Enforcement Act (CALEA) and the Lawful Access Needs of Federal, State, and Local Law Enforcement*, Press Release, FBI National Press Office, released September 8, 2004. (“FBI Press Release”)

This theme was echoed in recent FBI testimony before the House Subcommittee on

Telecommunications and the Internet:

[W]e have seen a truly commendable effort on the part of CableLabs, an industry trade consortium representing many cable companies, along with Time-Warner, Comcast, Cablevision and Cox Communications, to develop and publish a set of technical standards which, on their face, meet law enforcement needs with regard to electronic surveillance capabilities. This standard was developed in a spirit of cooperation which began by recognizing the legitimacy of law enforcement's needs and duties and the unique position industry is in to ensure that our public safety and national security missions are fulfilled.⁴

B. The Cable Industry Supports the Applicability of CALEA to VoIP Services as a Matter of Law.

The cable industry has also cooperated to develop new legal approaches to CALEA issues in response to changing and evolving technology. Earlier this year, the cable industry expressly supported the LEAs' view that the term "telecommunications carrier" is defined differently for purposes of CALEA than it is for purposes of Title II of the Communications Act.⁵ The LEAs had asked the Commission to issue a declaratory ruling determining – without awaiting the outcome of the Commission's *IP-Enabled Services* rulemaking – that CALEA applied to various kinds of IP telephony as well as to cable modem service and other forms of high-speed Internet access. *Most communications industries urged the Commission to reject the Administration's requests. The cable industry did not.*

⁴ Statement for the Record of Marcus C. Thomas, Deputy Assistant Director, Investigative Technology Division, Federal Bureau of Investigation, Before the United States House of Representatives, Committee on Energy and Commerce, Subcommittee on Telecommunications and the Internet, Washington, D.C., September 8, 2004, at 9.

⁵ Reply Comments of the National Cable & Telecommunications Association, RM-10865, filed April 27, 2004. ("NCTA Reply Comments")

In Reply Comments in that proceeding (which we incorporate by reference in this proceeding), the cable industry supported the issuance of a declaratory ruling by the FCC that providers of VoIP telephony are properly viewed as “telecommunications carriers” for purposes of CALEA, subject to two qualifications. First, the FCC should include within the scope of its ruling all similarly-situated providers of Broadband Telephony, including services like Vonage and AT&T’s CallVantage. Second, the Commission should make clear that, when services like Vonage and AT&T’s CallVantage are provided over the facilities of cable operators or other companies, the responsibility for complying with CALEA lies with the Broadband Telephony provider, not the facilities owner.

We went on to show that a Commission decision on the applicability of CALEA to VoIP need not, and should not, prejudge the classification issues raised in the *IP-Enabled Services* rulemaking, since CALEA defines “telecommunications carrier” differently than does the Communications Act: under CALEA, the term includes any provider of “wire or electronic switching or transmission service” if the Commission finds (1) “that such service is a replacement for a substantial portion of the local exchange service” and (2) “it is in the public interest to deem such person or entity to be a telecommunications carrier for purposes of this title.”⁶ In the *NPRM*, the Commission has adopted this approach,⁷ which permits the Commission to pursue its deregulatory policies with respect to advanced communications

⁶ CALEA, § 102(8)(B)(ii), 47 U.S.C. § 1001(8)(B)(ii). CALEA’s exemption of “information services” does not mean, as some commenters have suggested, that if the Commission subjects VoIP to CALEA, it may not classify VoIP as an information service for purposes of the Communications Act. That suggestion is wrong if for no other reason than that the Commission is free to define “information service” more narrowly under CALEA than under the Communications Act, in recognition of the two statutes’ distinct purposes. See NCTA Reply Comments at 2-3. *NPRM* at ¶¶ 50-51.

⁷ *NPRM* at ¶¶ 40-46.

services without hindering the law enforcement community in its efforts to conduct lawful surveillance in a changing technological context.

C. Applying CALEA to Broadband Internet Access Services Raises Technical Issues Distinct From Those Affecting VoIP.

In our Reply Comments, the cable industry supported the issuance of an NPRM addressing whether Broadband Access should be made subject to CALEA in due course. But we cautioned:

The ultimate decision on the merits here, however, raises more complex issues. Until now, there has never been substantial reason to expect that cable modem service might ever be subjected to CALEA. Thus, there has been little investigation or debate concerning the development of CALEA-related technical requirements for the equipment that cable operators use to provide the service. Making CALEA immediately applicable to cable modem service, therefore, is neither workable nor fair.⁸

As we emphasized in our prior filing, if the Commission eventually decides that cable modem service should be brought within CALEA's reach, it may do so without abandoning its prior holding that cable operators providing cable modem service do not provide a "telecommunications service" for purposes of the Communications Act. Just as the Commission may subject Broadband Telephony to CALEA without prejudging the classification issue under the Communications Act, so the Commission need not repudiate its 2002 *Declaratory Ruling* in the *Internet over Cable* proceeding that cable modem service is an interstate information service by making cable modem service subject to CALEA.⁹

Because the cable industry agrees with LEAs that VoIP may legally be subject to CALEA without impacting its regulatory classification and that – as a practical/technical matter – cable's

⁸ NCTA Reply Comments at 3.

⁹ *Id.* at 2-3.

VoIP services can be made CALEA-compliant through use of the CableLabs' PacketCable™ Electronic Surveillance Specification, and because we believe the question of CALEA's applicability to Broadband Internet Access will be fully vetted in other comments, we focus these comments on *technical concerns* over applying CALEA to cable modem service.

II. CABLE CAN PROVIDE A NUMBER OF THE CAPABILITIES DISCUSSED IN PARAGRAPH 66 OF THE NPRM.

The application of CALEA to broadband access presents different issues than the application of CALEA to VoIP. The *NPRM* recognizes as much in paragraph 66:

There are potentially several kinds of information about broadband access service that Law Enforcement may seek under section 103's requirements. For broadband access these potentially include, but are not necessarily restricted, to the following: (1) information about the subject's access sessions, including start and end times and assigned IP addresses, for both mobile and fixed access sessions; (2) information about changes to the subject's service or account profile, which could include, for example, new or changed logins and passwords; and (3) information about packets sent and received by the subject, including source and destination IP addresses, information related to the detection and control of packet transfer security such as those in Virtual Private Networks ("VPNs"), as well as packet filtering to favor certain traffic going to or from certain customers. For VoIP, the concept of "call" seems well understood, and we might expect call-identifying information to include who called whom when for how long, and concepts similar to call-identifying information for circuit-mode calls.

As the *NPRM* suggests, and as we discuss below, proper application of the statutory term "call-identifying information" for broadband services,¹⁰ and even the notion of a "call" itself," will require some guidance. Even so, cable technology is capable of offering significant support for lawful broadband surveillance.

It is appropriate at the outset to highlight some differences between the application of CALEA to VoIP, as compared to broadband access. VoIP, in its current form, offers subscribers

¹⁰ *NPRM* at ¶ 67.

telephone-like features that are readily identifiable with telephony service. Broadband access, however, does not have technical characteristics that map easily to CALEA requirements relating to call-identifying information. These voice-specific items include both call content and the “punch list” capabilities defined for VoIP: information on subject initiated conference calls; a means to correlate call identifying information with call content; subject initiated dialing and signaling; in band/out of band signaling; party hold/join/drop; and dialed digit extraction. In addition, broadband access has been in existence for much longer than VoIP, making it much more challenging to add capabilities without significantly modifying the network.

Even so, cable is able to provide a level of broadband access surveillance that addresses concerns stated in paragraph 66 of the *NPRM*. These include: (1) certain information about the subject’s “access sessions;”¹¹ (2) information about changes to the subject’s service or account profile, which could include new or changed logins and passwords; and (3) information about packets sent and received by the subject. We emphasize that this discussion relates to current and potential CALEA *capabilities*. Actual provision of this information is, of course, subject to LEAs’ lawful authority to obtain it by subpoena or otherwise and the privacy considerations mandated in CALEA.¹²

¹¹ Although the *NPRM* discusses IP addresses for both mobile and fixed access sessions, such discussion is not relevant to Cable modem service, which is always on and not mobile. As noted *infra*, some clarification of the non-statutory term “access session” will be required as the development of an actual broadband surveillance specification proceeds.

¹² As NCTA explained in its Reply Comments, both as a policy matter and as a technical matter, it is inappropriate to look to cable operators to provide surveillance information with respect to VoIP services offered by third parties, in which the cable operator’s role is simply to provide a connection to the Internet. This same principle applies to other services that might be enabled by the presence of a broadband connection, but which are fundamentally provided by, and under the control of, third parties. See NCTA Reply Comments at 5-6.

A. Cable Can Deliver Certain Information About Subjects' Access Sessions.

As to a subject's access sessions, start and end times and assigned IP addresses, cable operators can currently deliver to LEAs all packets sent and received by a cable modem in some tangible form (for example, on a tape drive, a hard disk drive, or other storage media) subject to operators' abilities to store the volume of packets requested. In addition, cable operators may be able to deliver all packets sent or received by a cable modem in real time, that is, as the packets are actually sent or received. As described below, however, this will depend upon resolution of the following technical issues: (1) sufficient capacity in the packet switch to mirror surveillance subjects' usage; (2) sufficient bandwidth for the cable operator to deliver the associated stream of packets; and (3) sufficient LEA bandwidth to receive the packet stream.

Cable operators may also be able to provide LEAs with the IP address assigned to a customer. This may, however require changes to existing cable network deployments to map the IP address assigned to a particular CPE device to a subscriber account. Moreover, in the broadband context, IP addresses are normally assigned for a period of time that can range between days and weeks. For this reason, providing LEAs with a subject's IP address without the associated subscriber identification over time will likely be of limited usefulness.

B. Cable Can Provide Information about a Subject's Service and Account Profiles.

Cable operators currently can provide some information about changes to the subject's service or account profile stored and used by the cable operator in providing its services. This could include, for example, information about changes to these profiles, and new or changed cable-supplied logins and passwords.

Cable operators could also provide information about “service profiles” (*i.e.*, the general information required to provide a cable operator’s service to the subject). In addition, cable operators could provide LEAs with a subject’s email addresses to the extent such addresses are provided by the cable operator.¹³ Information regarding account and login information for services not offered by the cable operator are not visible to the cable operator, and so could not be provided.

C. Cable Can Provide Law Enforcement Agencies Information About Packets Sent and Received by the Subject.

Today, with appropriate legal authorization under the terms of the Electronic Communications Privacy Act (“ECPA”), cable operators provide LEAs with storage media that contain complete information about packets sent and received by the subject; this necessarily involves source and destination IP addresses.¹⁴ As a result, providing such information is certainly technically feasible in the abstract, although CALEA differs from ECPA in certain ways that will undoubtedly affect the content of a final CALEA surveillance specification.¹⁵ Out of concern for subscriber privacy, a cable operator providing broadband access services does not inspect specific IP sessions, such as virtual private networks, web browsing, streaming media, or other types of sessions as part of its routine business operations.

¹³ This would not include information on email addresses provided by a third party, such as Yahoo or Google, as the cable operator would not have any information on such email addresses.

¹⁴ Cable operators are not able to provide the additional information requested in ¶ 66, namely “information related to the detection and control of packet transfer security such as those in VPNs, as well as packet filtering to favor certain traffic going to or from certain customers” as operators are unable to decrypt VPNs and do not use packet filtering to favor Internet traffic.

¹⁵ For example, in the ECPA context, information is often provided after the fact, while CALEA often requires that information be provided in real time. Particularly in light of the amount of information transmitted using high-speed Internet access services, this consideration can materially affect the content of a CALEA surveillance specification. *See USTA v. FCC*, 227 F.3d. 450, 465-66 (D.C.Cir. 2000).

The cable operator cannot provide content information for IP sessions for encrypted services provided by a third-party. Encrypted IP sessions which ride over the cable operator's network are not accessible to the cable operator, as the operator would not have any of the keys necessary to decrypt the content. Therefore, while a cable operator may be able to inform LEAs about the transmission and receipt of packets, a cable operator cannot provide specific information about the services accessed.

III. ADDITIONAL GUIDANCE IS REQUIRED ON CERTAIN MATTERS DISCUSSED IN THE *NPRM*.

Paragraph 66 of the *NPRM* broadly describes the kinds of capabilities that LEAs might need in connection with broadband services, such as cable modem service. The cable industry stands ready to work with law enforcement to develop effective, practical means to meet lawful surveillance needs in this context. As a first step in that effort, and based on the statements in paragraph 66 of the *NPRM*, it is clear that lawful surveillance of broadband services raises some technical issues that are not raised in the context of voice services. Additional guidance is needed with respect to these issues before a meaningful broadband surveillance specification can actually be developed.

NCTA emphasizes that these issues do not, at least at this juncture, appear to present any insurmountable barriers to the implementation of reasonable lawful surveillance mechanisms. Even so, in practical terms, the cable industry and its suppliers will not be in a position to know how to craft a workable specification without additional guidance.¹⁶

¹⁶ Of course, as the detailed technical work of developing an actual specification gets underway, other issues will likely arise that will take a certain amount of time and effort to resolve.

A. Clarification of the Definition of “Access Session” in the Broadband Context Will be Required to Develop a Workable Surveillance Specification.

First, the *NPRM* speaks in terms of providing information with respect to a particular “access session.”¹⁷ *NPRM* at ¶ 66. The concept of an “access session” is well-defined in the context both of voice services (essentially, an “access session” is a telephone call) and of dial-up Internet access (each call to an ISP constitutes a separate “access session”). The “always on” nature of broadband services, however, makes it unclear what is actually intended by the term “access session” for broadband. This is because, in the normal course, a cable modem service subscriber connects the cable modem to the cable system, plugs it in, turns it on, and, essentially, never turns it off. Given this fundamental difference between dial-up and broadband, it is unclear how the term “access session” applies to broadband service.¹⁸

¹⁷ The *NPRM* refers to “access session” (which is not a statutory term) without providing a clear definition of that term. Some additional clarity will be required in order to develop a workable surveillance specification.

¹⁸ The period of time that a particular IP address is assigned to a cable modem device does not appear to correspond to an “access session.” IP addresses for cable modems and the Customer Premise Equipment (“CPE”) behind them are allocated using Dynamic Host Configuration Protocol (“DHCP”). DHCP can allocate IP addresses that can remain in effect for times that can range between days and weeks. This is to be contrasted with the normal practice by which dial-up ISPs assign IP addresses to dial-in users. There, a caller is assigned an IP address from the ISP’s address block at the beginning of a dial-in session; the address is returned to the pool of assignable addresses when the call to the ISP terminates. In that context, the period of time that a particular IP address is assigned to a particular user would, indeed, appear to correspond with an “access session.” As noted in Section II, to the extent that LEAs have a need to know when a particular cable modem is assigned a new or different IP address, that is almost certainly feasible. Unfortunately — and unlike the situation with connections to dial-up ISPs — it does not appear that this would provide LEAs with the information that the Commission seems to have in mind with the term “access session.” Therefore, as noted above, additional guidance is required.

B. Both Service Providers and Law Enforcement May Face Bandwidth Constraints Due to the Huge Amounts of Data Potentially Subject to Surveillance.

A second issue, related to the “always on” nature of broadband services but worthy of separate comment, is the sheer volume of data that can potentially be exchanged using such services. This affects the practical design of any lawful surveillance specification for broadband in two ways. First, depending on the capacity requirements for surveillance of broadband usage, it may prove technically challenging to design a surveillance methodology that does not interfere with the operation of the service itself. Second, using an overly “generous” capacity level may actually overwhelm the ability of the affected LEAs to process the data they might receive.

For example, suppose that in a particular area a cable operator has 20,000 cable modem service subscribers. As a point of reference, the PacketCable surveillance specification for voice communications, based upon the capacity for wireline surveillance, states that the system must be able to handle simultaneous surveillance of a maximum of 5% of VoIP subscribers. Applying that same 5% criterion to broadband services in a 20,000-subscriber system would imply a need to be able to simultaneously monitor 1,000 broadband subscribers, each of whom could, at least in theory, be simultaneously downloading or uploading files at a rate of 1 megabit per second or more. This implies a data rate of more than a gigabit per second.

Cable operator routers would need to have sufficient capacity to process this additional data to create a “mirror” of the packets sent to and received by surveillance subjects; otherwise, the service could well degrade (slow down) and might even tend to “tip off” subjects that they are under surveillance. In addition, assuming that the cable operator’s network can handle the

mirroring function, a data link to law enforcement on the order of two OC-12s (that is, 24 DS3s, or 1.038 gigabits/second) would be required.

By contrast, if 1,000 VoIP users were all talking at the same time, the total bit rate would not fill up a single DS3. Unlike VoIP, broadband service is not limited in its intrinsic bandwidth. As recent history has shown, demand for ever-higher subscriber service tiers from 1.5 Mbps up to 9 Mbps and higher continues to grow. This means that the bandwidth required to monitor any given percentage of broadband subscribers will grow proportionately over time.

The vastly different bandwidth requirements associated with surveillance of broadband versus voice illustrate the challenge in designing a specification. In the voice context, the cable industry viewed it to be very unlikely that anything close to 5% of its customers would be subject to simultaneous surveillance. Even so, the technical consequences of specifying such a “generous” capacity assumption in that context were manageable, so there was no significant engineering downside to doing so. By contrast, simply assuming that “more capacity is better” in crafting a surveillance specification for broadband service could actually end up frustrating effective surveillance. It is therefore much more important, in the broadband surveillance context, to have a realistic assessment of LEAs’ capacity requirements – today and projected into the future – early in the process of developing the specification.

C. A Reasonable Compliance Period Will be Required.

NCTA emphasizes again that we do not raise the issues above as insurmountable barriers to establishing meaningful and useful surveillance methods for broadband service. Instead, the concern is that without clarification with respect to these issues, the industry will not have sufficient guidance as to what a broadband surveillance specification should actually do. Such a

situation would inevitably foster disputes as well as delay the completion of the specification. For this reason, NCTA respectfully requests that the Commission and/or affected LEAs provide such guidance at the earliest practicable time.

The existence of these (and possibly other) issues where guidance is needed, however, does serve to emphasize a final point. Because at present there are no surveillance specifications for broadband services, the Commission will need to establish a reasonable period for developing and implementing such specifications, assuming that it concludes that CALEA applies to such services. It would be unfair to hold the industry at risk for potential penalties for non-compliance with CALEA¹⁹ without first establishing a reasonable period during which the parameters of surveillance requirements can be defined and associated system and equipment specifications developed.

IV. CABLELABS QUALIFIES AS AN "INDUSTRY ASSOCIATION OR STANDARD-SETTING ORGANIZATION" UNDER CALEA SECTION 107(a)(2).

Paragraph 80 of the *NPRM* questions whether there is a need to define what constitutes publicly available technical requirements or standards adopted by an industry association or standard-setting association necessary to establish a CALEA “safe harbor.” The *NPRM* raises the concern that any organization could publish a set of technical specifications and claim that such specifications are a “safe harbor.” Near the conclusion of Paragraph 80 of the *NPRM* the question of CableLabs’ ability to establish a “safe harbor” is expressly raised.

CALEA states that if a telecommunications carrier, manufacturer or support service provider is in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization, such carrier, manufacturer or support

¹⁹ See CALEA, § 108(a), 18 U.S.C. § 2522(c)(enforcement orders relating to CALEA).

service provider is in compliance with CALEA.²⁰ It is not necessary here to define what entities might or might not qualify for this function. Whatever might be the case with others, CableLabs is precisely the type of organization that Congress had in mind in Section 107(a)(2) of CALEA.

As noted in the *NPRM*, CableLabs is an industry association – a consortium of cable operators whose function is to handle a variety of technical matters for the industry. CableLabs, with the assistance of cable operators and equipment manufacturers creates publicly available technical requirements. CableLabs’ members include operators of cable systems serving over 80% of United States cable subscribers. In addition, the technical output of CableLabs’ activities – technical specifications, etc. – are available to, and used by, all of the industry. Whatever the status of other organizations, therefore, it is clear that CableLabs, as an industry association creating publicly available technical requirements, meets the CALEA standard in Section 107(a)(2) for an organization that may create a “safe harbor.”

The Commission’s concern in raising this issue may be that a less-than-technically-astute industry group might try to generate a facially deficient specification and declare it to be a “safe harbor.” That is manifestly not a problem in the case of CableLabs. Not only have LEA representatives participated with CableLabs in developing the various iterations of the PacketCable specification. As noted earlier, LEAs have expressly and publicly praised CableLabs for its efforts in this area.²¹

²⁰ CALEA, § 107(a)(2). 47 U.S.C. § 1006(a)(2).

²¹ See notes 3 and 4 *supra*, and accompanying text.

Finally, the statute itself provides a means for addressing an inadequate CALEA compliance specification, irrespective of the entity that produced it. If a “safe harbor” created by any organization is deficient, LEAs or others may bring the matter to the attention of the Commission, which can cure the deficiency by modifying the specification/standard, and thereby solve the problem.

Given that the NPRM raises this issue and expressly mentions CableLabs, NCTA respectfully requests that the Commission expressly state that CableLabs *is* an organization qualified to create CALEA specifications that qualify for “safe harbor” treatment under Section 107(a)(2).

CONCLUSION

The cable industry stands ready to work with the Commission and law enforcement on making cable's VoIP services CALEA compliant and to explore ways to do the same for cable modem service, regardless of the Commission's ruling on the legal issues raised in this proceeding. To fully do so, the Commission and LEAs need to provide additional guidance with respect to certain issues raised in the *NPRM* and discussed in these Comments. In addition, the Commission should make clear that CableLabs qualifies as an "Industry Association or Standard Setting Organization" under Section 107(a)(2) of CALEA.

Respectfully submitted,

/s/ Daniel L. Brenner

Of Counsel:
Christopher W. Savage
Cole, Raywid & Braverman, LLP
1919 Pennsylvania Avenue, N.W.
Suite 200
Washington, D.C. 20006
(202) 659-9750

November 8, 2004

Daniel L. Brenner
Neal M. Goldberg
Michael S. Schooler

National Cable & Telecommunications
Association
1724 Massachusetts Avenue, N.W.
Washington, D.C. 20036
(202) 775-3664