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

In the Matter of	)	
	)	
Communications Assistance for	)	ET Docket No. 04-295
Law Enforcement Act and	)	
Broadband Access and Services	)	RM-10865

TO: The Commission

COMMENTS OF THE COALITION FOR REASONABLE RURAL BROADBAND CALEA COMPLIANCE

Gerard J. Duffy
Blooston, Mordkofsky, Dickens, Duffy & Prendergast
2120 L Street, NW (Suite 300)
Washington, DC 20037
Telephone: (202) 659-0830
Facsimile: (202) 828-5568

Dated: November 8, 2004

Table of Contents

Summary ii
COMMENTS OF THE COALITION FOR REASONABLE RURAL BROADBAND CALEA COMPLIANCE 1
Rural Telephone Companies Have Been Furnished No Guidance Regarding Compliance with CALEA Packet-Mode Surveillance Requirements 2
Denying Packet-Mode Extensions and Waivers Will Discourage or Effectively Prohibit the Provision of Broadband Services 7
A Separate FCC Enforcement Program Would Exacerbate the Adverse Impact Upon the Provision of Broadband Services 13
Trusted Third Party Alternatives Require Clarification 16
Conclusion 17

Summary

The Coalition for Reasonable Rural Broadband CALEA Compliance ("Coalition"), a group of rural telephone companies that have made substantial investments in broadband facilities, oppose the Commission's proposed termination of CALEA Section 107(c) extensions, implementation of stringent requirements for CALEA Section 109(b) waivers, and initiation of its own CALEA enforcement program. If adopted, these proposals will discourage or effectively prohibit the deployment of broadband services by rural telephone companies that lack access to specific and reasonably affordable CALEA upgrades.

Coalition members and other rural telephone companies are ready and willing to comply with packet-mode CALEA requirements in the same manner they generally have complied with circuit-switched CALEA requirements. However, they have not yet received clear guidance from this Commission, the FBI or their equipment vendors as to the hardware or software upgrades, if any, they need to acquire and install.

Until specific CALEA solutions are readily available for rural carriers, they risk substantial CALEA penalties if they deploy or provide DSL and other packet-mode services without obtaining CALEA Section 107(c) extensions or CALEA Section 109(b) waivers. The Commission's proposed elimination of Section 107(c) extensions for packet services and restriction of Section 109(b) waivers contravene the fundamental CALEA policy of encouraging the provision of new technologies and services.

CALEA Section 107(c) can be read to limit the "prior to the effective date of Section 103" restriction to circuit-switched equipment installed or deployed after October 25, 1998, and

to permit extensions for packet-mode and other new equipment and services developed after that date. If the Commission and FBI want to accelerate packet-mode CALEA deployment in an effective and equitable manner, they can employ CALEA Section 106 to pressure manufacturers directly to provide timely and affordable CALEA solutions.

Likewise, CALEA Section 109(b) can be read to permit waivers on the basis of one or more of the provision's eleven enumerated factors (including "encouragement of the provision of new technologies and services" and "the financial resources of the telecommunications carrier"). It is neither reasonable nor necessary to employ stringent negotiation and cost data standards to restrict such waivers.

Finally, CALEA Sections 108 and 201 deal comprehensively with the enforcement of CALEA requirements by the courts. There is no need for the Commission to adopt and implement its own CALEA enforcement program.

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

In the Matter of	)	
	)	
Communications Assistance for	)	ET Docket No. 04-295
Law Enforcement Act and	)	
Broadband Access and Services	)	RM-10865

TO: The Commission

COMMENTS OF THE
COALITION FOR REASONABLE RURAL BROADBAND CALEA COMPLIANCE

The Coalition for Reasonable Rural Broadband CALEA Compliance[1] ("Coalition") hereby submits its comments with respect to the Commission's Notice of Proposed Rulemaking and Declaratory Ruling (Communications Assistance for Law Enforcement Act and Broadband Access and Services), FCC 04-187, released August 9, 2004 ("NPRM").

The Coalition is comprised of rural telephone companies that have made substantial investments in broadband facilities, and that desire to continue to deploy and operate broadband facilities and services in their rural service areas. All presently provide Digital Subscriber Line ("DSL") facilities and services over which increasing numbers of their customers may access the Internet, or otherwise send and receive packet-mode messages.

Coalition members are ready and willing to comply with packet-mode Communications Assistance for Law Enforcement Act ("CALEA") surveillance capability requirements, and to acquire, install and deploy reasonably affordable hardware and/or software upgrades that are identified by appropriate authorities as necessary to achieve compliance. However, they have

[1] The Coalition is comprised of the following rural telephone companies: Harrisonville Telephone Company; Lavaca Telephone Company, Inc., d/b/a Pinnacle Communications; Madison County Telephone, Inc.; Midstate Communications, Inc.; and Santel Communications Cooperative, Inc.

not received clear guidance from this Commission, the Federal Bureau of Investigation ("FBI"), or their equipment vendors as to the hardware and/or software, if any, they need to acquire and install in order to comply with the CALEA surveillance capability requirements for packet-mode communications. They believe that many other rural telephone companies suffer from the same lack of clarity and guidance. In light of this uncertainty, the Commission's proposed termination of CALEA Section 107(c) extensions, proposed implementation of stringent requirements for CALEA Section 109(b) waivers, and proposed initiation of its own CALEA enforcement program will discourage broadband deployment by rendering rural telephone companies subject to substantial forfeitures if they continue to invest in and provide broadband services to their rural customers.

Rural Telephone Companies Have Been Furnished No Guidance
Regarding Compliance with CALEA Packet-Mode Surveillance Requirements

The majority of rural telephone companies have complied with most or all CALEA circuit-switched surveillance capability requirements.[2] Coalition members are ready and willing to comply with CALEA packet-mode surveillance capability requirements once the Commission, the FBI and/or their equipment vendors inform them what additional equipment, if any, they need to acquire and install to achieve compliance (provided, of course, that such equipment is readily available and affordable).

The problem is that no clear and specific guidance regarding CALEA packet-mode compliance has been forthcoming from this Commission, the FBI or equipment vendors.

[2] In some instances, rural telephone companies with Nortel DMS-10 switches have requests pending for extension of the dialed digit extraction "punch list" capability due to their inability to install the necessary NT4T50 card without expensive hardware upgrades. In other instances, rural telephone companies have sought extensions because of their inability to obtain CALEA upgrades for certain makes and models of switches.

It does not appear to be an insurmountable technical problem to isolate and intercept packets sent to or from a particular Internet Protocol ("IP") address, and to deliver copies of such packets to law enforcement. It may be a significantly more difficult and complex problem to implement a pen register or trap and trace on packet-mode traffic without impairing privacy rights, or to isolate and access "punch list" (e.g., party hold/join/drop and subject-initiated conference calls) and call identifying information with respect to packet-mode communications.

The relatively small staffs of rural telephone companies generally lack the expertise and resources to develop their own CALEA standards or solutions to resolve most or all of these technical problems. In particular, the relatively small size and buying power of rural telephone companies give equipment vendors little or no incentive to develop CALEA solutions on their behalf or to produce CALEA solutions that they design. Rather, rural telephone companies need to be able to purchase and install commercially available CALEA hardware and/or software upgrades that are compatible with the commercially available routers and/or digital subscriber line access multiplexers ("DSLAMs") over which they provide packet-mode services.[3]

To date, the Coalition is aware of no clear statement or information from this Commission or the FBI detailing precisely what rural telephone companies need to do to render their packet-mode facilities CALEA compliant. Undersigned counsel has asked FBI representatives whether it is possible to install and run the DCS1000 (formerly Carnivore) packet sniffing program on most or all existing routers, and whether this means that such routers are presently CALEA-compliant without the need for any further hardware or software upgrades. He has been informed that it "is not that simple," but has not obtained clear guidance whether all, some or no existing routers could comply with CALEA by accommodating the DCS1000

[3] Whereas the packet-mode networks of many rural telephone companies are comprised of routers and DSLAMs, some rural telephone companies employ ATM switches.

program and its successors. Or, in the event that substantial numbers of existing routers require hardware and/or software upgrades to comply with CALEA surveillance capability requirements, it is not clear what types of upgrades are necessary for compliance.

The Coalition believes that DSLAMs are relatively simple frequency splitters, and that it is not technically feasible or practicable to install interception or call identifying information functions in DSLAMs. However, whereas no FBI or Commission representative has expressed disagreement to undersigned counsel with respect to this presumption, neither agency has clarified whether or not DSLAM upgrades are required at this time.

The NPRM claims that it "is simply not true that no packet-based standards have been developed by standards committees," and cites as proof a standard for intercepting and delivering packet content to law enforcement that was included in J-STD-025. NPRM, at note 226. However, it is not clear whether this is the only CALEA standard with which packet-mode service providers must comply at this time, or whether there are additional packet-mode standards regarding call identifying information and/or "punch list"-type functions applicable at this time or in the near future. More important, the Coalition is aware of no hardware or software that they can be purchased and installed to implement the J-STD-025 packet content standard and/or any additional or future CALEA packet-mode standard in routers (or DSLAMs).

Equipment vendors also have provided virtually no meaningful guidance. When asked about potential CALEA solutions and upgrades during the months prior to the initial November 19, 2001 packet-mode compliance deadline, the three most common DSL vendor responses appear to have been: (1) what is CALEA?; (2) we know about CALEA but are not subject to it; and (3) we are working on a CALEA solution, but don't know if or when it will be available. By the November 19, 2003 deadline (extended to January 30, 2004), vendors had become aware of

CALEA, but were no more forthcoming with CALEA compliance information, solutions or upgrades. Many rural telephone companies were unable to obtain written responses from their DSL equipment vendors regarding CALEA compliance, and some could not even get their telephone inquiries returned. Even when responses in writing were obtained from vendors, they generally were worded to minimize potential vendor exposure to liability under CALEA Section 106 and contained little useful CALEA compliance information.

For example, Cisco Systems, the vendor for a large portion of the routers used by rural telephone companies providing DSL services, furnished the attached letter in response to a number of inquiries (Exhibit A). Cisco began by noting that it "has been developing and testing the ability to intercept IP packets based on source/destination IP address on several of its product platforms." It then qualified this statement by indicating that its "products" must be utilized in conjunction with unidentified "third party mediation device equipment" in order to effect the interception of IP traffic. It further qualified its statements by indicating that the provider's "ability to effectively conduct the interception of IP traffic will depend on the specific configuration of your network and service they are providing to their customers." Notwithstanding the foregoing qualifications, Cisco then completely abrogated any responsibility for the CALEA functionality of its routers by declaring that it "makes no representations or warranties as to whether or not the platforms listed above will permit your client's compliance with their "packet-mode' CALEA requirements." Cisco then passed the buck to rural telephone company attorneys (many of whom, like undersigned counsel, went to law school because they lacked technical proficiency to analyze anything much more complex than a can opener), and indicated that its router customers should "consult their own legal counsel to determine their specific obligations pursuant to [CALEA]." Finally, Cisco advised its router customers that they

"may also want to consider contacting a third party mediation device vendor, such as Verint or SS8, regarding the possibility of purchasing alternative 'packet-mode' CALEA functionalities compatible with the listed device(s) and/or system(s) that they have purchased from our company."

In short, Cisco was unwilling or unable to tell its router customers specifically what they need to do to upgrade their Cisco Series 72xx, 75xx, 100xx and/or 366x routers to comply with CALEA. Rather, Cisco's qualifications and suggestions to look elsewhere appear to indicate that it has no clear or specific CALEA solution and does not know if or when it will develop one.

This problem is not unique to Cisco. The attached January 30, 2004 letter from Redback Networks (Exhibit B) indicates that it was "currently developing/investigating cost-effective, near-term, and, in some cases, extensible long-term lawful-intercept solutions" and that "it appears that full CALEA compliance will involve a still-to-be-defined combination of service provider specific infrastructure and network equipment vendor solutions tailored to that infrastructure." In short, Redback also had no clear or specific CALEA solution and could give no indication when one might be forthcoming. Likewise, DSLAM vendors have issued a variety of statements regarding CALEA compliance (Exhibit C), the common element of which is that they have developed no CALEA hardware or software for use with their equipment.

To reiterate, Coalition members and other rural telephone companies are ready and willing to purchase and install affordable hardware and/or software that will enable their DSL networks to comply with applicable CALEA packet-mode surveillance capability requirements. They do not have the resources or capabilities to develop their own CALEA packet-mode standards or solutions, or to partner with equipment vendors to develop and manufacture their own CALEA hardware or software. Rather, if the Commission, the FBI and/or their equipment

vendors will tell them, or give them enough information to determine, what specific hardware or software upgrades they need to acquire to comply with CALEA, they will purchase and install that equipment. To date, such information has not been forthcoming.

Denying Packet-Mode Extensions and Waivers
Will Discourage or Effectively Prohibit the Provision of Broadband Services

The fundamental purpose of CALEA was to preserve the government's ability to intercept communications involving advanced technologies while protecting the privacy of communications and without impeding the introduction of new technologies, features and services. H.R. Rep. No. 103-827, 103d Cong., 2d Sess., Pt.1, at 13 (1994). The prohibition against impeding the introduction of new technologies, features and services is repeated throughout the statute. CALEA Section 103(b)(1)(B) expressly limits assistance capability requirements to preclude law enforcement from prohibiting "the adoption of any equipment, facility, service, or feature by any provider of a wire or electronic communication service." CALEA Section 107(b) requires any technical requirements or standards established by the Commission to "serve the policy of the United States to encourage the provision of new technologies and services to the public." Likewise, one of the eleven factors to be considered by the Commission in its evaluation of CALEA Section 109(b) waiver petitions is the same "policy of the United States to encourage the provision of new technologies and services to the public."

Until clear and specific CALEA packet-mode upgrades become available, potential penalties for CALEA non-compliance will discourage or effectively prohibit rural telephone companies and other small carriers from providing DSL, broadband Internet access, Voice over Internet Protocol ("VoIP") calling and other new broadband services unless they can obtain Section 107(c) extensions or Section 109(b) waivers. Rural carriers lack the staff and resources

to develop their own CALEA standards and solutions, the economic power to negotiate system-specific CALEA solutions with their vendors, and the profitability to pay the $10,000 per day statutory fine for CALEA non-compliance (and/or any forfeiture the Commission may adopt and impose). Until they can obtain appropriate CALEA upgrades at reasonable prices, rural carriers have no viable option other than to obtain CALEA Section 107(c) extensions or CALEA Section 109(b) waivers, or to cease or restrict their offering of packet-mode services that are subject to CALEA requirements.

Coalition members are very concerned with the Commission's tentative conclusions: (a) that Section 107(c) extensions are not available to cover equipment, facilities or services installed or deployed after October 25, 1998, NPRM at par. 97; and (b) that Section 109(b) waivers will require detailed and stringent showings, *inter alia*, of precisely identified costs, public safety and national security impacts, and due diligence that most carriers will find very difficult (and, in most cases, impossible) to satisfy, NPRM at par. 98-99. If it adopts and implements these tentative conclusions and virtually eliminates CALEA Section 107(c) extensions and CALEA Section 109(b) waivers for packet-mode services, the Commission will discourage or effectively prohibit rural telephone companies and other small carriers from offering DSL and other packet-mode services that are subject to CALEA requirements.

The Commission states that making Section 107(c) extensions and Section 109(b) waivers difficult to obtain and subjecting carriers to immediate enforcement action, will "encourage carriers to press for the development of CALEA standards by industry-staffed committees and for solutions from manufacturers." NPRM at par. 99. It notes that its proposed interpretations of Sections 107(c) and 109(b) "clearly impose great responsibility on carriers to

actively and consistently advocate for the development of technical standards and solutions." Id., at par. 100.

Rural telephone companies and other small carriers generally lack sufficient staff resources and expertise to participate significantly on industry standard-setting committees, and sufficient buying power to negotiate the design, development and/or production of specific CALEA solutions with manufacturers and other vendors. As noted above, during the preparation of the Section 107(c) extension petitions filed in November 2003 and January 2004, it was extremely difficult for many rural telephone companies to obtain even a specific CALEA compliance letter from their DSL equipment vendors. Rather, many rural telephone company petitioners were forced to rely upon general CALEA statements on vendor websites and upon letters furnished by their vendor to larger carriers or carrier groups. Requiring small carriers to submit detailed information about their CALEA "discussions and negotiations" with manufacturers who often do not return their calls will ensure that they receive no compliance relief and force them to choose between terminating their packet-mode services and risking substantial CALEA penalties.

Penalizing large or small carriers as an indirect device to pressure equipment manufacturers to develop and market CALEA solutions is inequitable and inefficient public policy. CALEA Section 106(b) requires manufacturers of telecommunications transmission and switching equipment (as well as providers of telecommunications support services) to make available, on a reasonably timely basis and at reasonable charges, the features or modifications necessary to permit carriers that use their equipment to comply with CALEA capability requirements. This provision can and should be employed directly with respect to manufacturers of routers and other packet-mode equipment to give them the requisite incentives to push the

industry committees they dominate to develop appropriate CALEA standards and to develop and market CALEA hardware and/or software incorporating such standards. Once manufacturers furnish reasonably priced CALEA packet-mode solutions, the need for Section 107(c) extensions and Section 109(b) waivers will be minimized.

The Coalition is aware of the wording of CALEA Section 107(c)(1), but does not believe that Congress intended to deny CALEA compliance extensions for all new and developmental services and equipment installed or deployed after October 25, 1998. This would require all new wire or electronic switching or transmission services to be fully compliant with CALEA on the day they are first offered, as well as all wire or electronic services that the Commission might subsequently find to be replacements for substantial portions of local exchange telephone service.

It is not feasible or practicable to require carriers, entrepreneurs and manufacturers to develop and implement CALEA solutions before introducing new services or equipment. This would impair, delay or prohibit the adoption of new services and equipment, and contravene the critical policy goal of encouraging the provision of new technologies and services to the public.

The more reasonable interpretation of CALEA Section 107(c)(1) is that the drafters were thinking about traditional circuit-switched equipment, facilities and services when they included the "prior to the effective date of Section 103" phrase. This is consistent with the legislative history, which indicates that "the scope of the legislation has been greatly narrowed," and that the "only entities required to comply with the functional requirements are telecommunications common carriers, the components of the public switched network where law enforcement agencies have always served most of their surveillance orders." H.R. Rep. No. 103-827, supra. It makes sense to require traditional circuit-switched equipment to be CALEA compliant when it

is installed or deployed after October 25, 1998, but it would inhibit innovation if this requirement were extended to encompass packet-mode and other equipment and services developed after October 1998.

The Coalition notes that numerous petitions for CALEA Section 107(c) extensions were filed with the Commission on or about November 19, 2001, and were accepted and allowed to remain pending until January 30, 2004 (during which time there were deemed to be provisional extensions). Neither the Commission nor the FBI challenged the propriety or validity of these petitions at the time they were filed or at any time during the twenty-six months they remained pending. In fact, the Commission issued a September 28, 2001 Public Notice establishing procedures for the filing of the November 2001 packet-mode petitions[4], and a subsequent November 19, 2003 Public Notice extending the provisional extensions accorded to the petitions to January 30, 2004[5]. Likewise, the FBI published a CALEA Flexible Deployment Assistance Guide, Second Edition (Packet-Mode Communications) in August 2001 for use in conjunction with the November 2001 extension petitions.

Likewise, numerous petitions for further Section 107(c) extensions were filed with the Commission during the period from November 2003 to January 30, 2004, and were accepted and remain pending to this date. Although the FBI did not extend its Flexible Deployment Assistance Program with respect to the November 2003 and January 2004 petitions, neither the FBI nor the Commission challenged the propriety or validity of these petitions at the time they were filed.

---

[4] *The Common Carrier and Wireless Telecommunications Bureaus Establish Procedures for Carriers to Submit or Supplement CALEA Section 107(c)(2) Extension Petitions, both Generally and with Respect to Packet-Mode and Other Safe Harbor Standards*, CC Docket No. 97-213, *Public Notice*, 16 FCC Rcd 17101 (2001) ("September 28, 2001 Public Notice").

[5] *The Wireline Competition and Wireless Telecommunications Bureaus Announce a Revised Schedule for Consideration of Pending Packet Mode CALEA Section 107(c) Petitions and Related Issues*, CC Docket No. 97-313, *Public Notice*, 22 FCC Daily Dig. 220 (released November 19, 2003)("November 19, 2003 Public Notice").

Even in their March 10, 2004 "Joint Petition for Expedited Rulemaking," the Department of Justice ("DOJ"), FBI and Drug Enforcement Administration ("DEA") did not advocate that packet-mode service providers be denied any and all further extensions. Rather, they proposed a stringent fifteen-month implementation period (with six-month and twelve-month benchmark filings) during which all packet-mode service providers would be required to become CALEA compliant, including the development of their own CALEA standards and equipment if industry standards and solutions did not emerge. *DOJ/FBI/DEA Petition*, pp. 40-53. Whereas the Coalition would have opposed the DOJ-FBI-DEA proposal because it placed an impossible burden upon small carriers, the Commission's proposal is even more onerous. It would eliminate CALEA Section 107(c) extensions for DSL and other post-October 25, 1998 equipment and services, and force small carriers to risk substantial penalties for CALEA violations if they invest in new packet-mode technologies and services.

The Commission's tentative conclusion to make CALEA Section 109(b) waivers difficult to obtain forecloses the alternative avenue of relief for rural telephone companies offering DSL and other broadband services. Vendors selling a few routers or DSLAMs to a rural telephone company are not going to engage in significant negotiations or discussions to develop a general or a system-specific CALEA solution for the carrier. Such vendors also will not provide small carriers with a thorough analysis of the precisely identified costs that might be necessary to upgrade their equipment to comply with CALEA.

The stringent showing proposed by the Commission will ensure that few, if any, CALEA Section 109(b) waivers will be granted to small carriers. This result is not mandated by Section 109(b), which can be read to permit determinations that CALEA compliance is not "reasonably achievable" on the basis of one or more of the eleven enumerated factors, including

"encouragement of the provision of new technologies and services to the public" and "the financial resources of the telecommunications carrier."

In sum, although the Commission recognizes that its tentative conclusions "could create potentially heavy burdens for small and rural carriers in particular," NPRM at par. 100, it offers no option that will encourage or allow them to continue deploying and providing DSL and other broadband services without risking substantial CALEA penalties until appropriate CALEA hardware and/or software upgrades become commercially available. The Coalition proposes that the Commission interpret the "prior to the effective date of Section 103" phrase in CALEA Section 107(c)(1) to restrict extensions only with respect to traditional circuit-switched equipment, facilities or services installed or deployed after October 25, 1998, and that it continue to accept petitions for CALEA Section 107(c) extensions for DSL and other new broadband equipment and services. In the alternative, the Commission should grant Section 109(b) waivers to permit small carriers to provide new technologies and services to the public until affordable CALEA solutions become reasonably available without risking crippling CALEA forfeitures.

A Separate FCC Enforcement Program Would Exacerbate The Adverse Impact Upon the Provision of Broadband Services

CALEA Section 108 and CALEA Section 201 (also known as 18 U.S.C. Sec. 2522) deal expressly and comprehensively with the enforcement of CALEA surveillance capability and capacity requirements. These provisions permit the court authorizing an electronic surveillance to issue a CALEA compliance order against a carrier or manufacturer unable to implement the surveillance, and to impose a civil penalty of up to $10,000 per day upon the carrier or manufacturer for violation of the compliance order. They permit the court to court to consider: (a) the nature, circumstances, and extent of the violation; (b) the violator's ability to pay; (c) the

violator's good faith efforts to comply in a timely manner; (d) the effect on the violator's ability to continue to do business; (e) the degree of the violator's culpability; and (f) the length of any delay in undertaking efforts to comply.

CALEA Sections 108 and 201 reasonably tie enforcement to specific instances where a surveillance order is issued, and a carrier required to be CALEA compliant cannot implement it because it has not installed the required CALEA capabilities or because its vendor has not furnished them. They authorize the court to take complete and effective action to compel compliance by carriers and their vendors, and to punish unreasonable and unexcused delays and failures to comply.

In light of the comprehensive nature of CALEA Sections 108 and 210, it is not necessary for the Commission to prescribe rules or to develop its own enforcement program to implement the CALEA capability and capacity requirements. Whereas Section 229(a) of the Communications Act gives the Commission authority to prescribe its own CALEA rules, it does not confer this power in cases where Commission rules are not necessary or would duplicate or conflict with enforcement responsibilities specifically given to the courts.

Moreover, a separate Commission enforcement program would further discourage rural telephone company investment in and provision of broadband services by rendering carriers liable for substantial CALEA forfeitures even when they have not received a surveillance order and have no prospect of receiving one within the foreseeable future. Sparsely populated rural areas generally are not good hiding places for terrorist, drug trafficking and other activities for which electronic surveillance may be deemed necessary.[6] Many rural telephone companies have not been served with a wiretap order for decades, and are likely to become aware of suspicious

[6] Whereas Posse Comitatus, Freemen, Branch Davidian and other groups have been active in rural areas, their presence is generally well known to local residents, including telephone company personnel.

local residents, visitors or activities well before law enforcement finds it necessary to initiate electronic surveillance. Hence, it may be feasible for some rural telephone companies to furnish DSL and other broadband services before CALEA-compliant hardware or software is available without incurring significant risk of CALEA violations and forfeitures because they know of no local residents or groups likely to become targets of electronic surveillance.

A separate Commission enforcement program would discourage all carriers from deploying and providing packet-mode services before CALEA solutions are available, whether or not they were likely to be served with a surveillance order. Carriers could be cited and fined for failure to implement CALEA solutions as a result of random Commission inspections and audits, even where there was no possibility that they might be required to implement a surveillance within the foreseeable future. This would exacerbate the disincentives and effective prohibitions against broadband investment and deployment that will result from the Commission's proposed elimination of CALEA Section 107(c) extensions and CALEA Section 109(b) waivers.

The Coalition recommends that the Commission reject a separate CALEA enforcement program as unnecessary, and allow the courts to continue to enforce CALEA capability and capacity requirements when carriers and manufacturers are unable to implement surveillance orders in a reasonable and timely manner.

Trusted Third Party Alternatives Require Clarification

The Coalition is willing to explore the feasibility of employing a "trusted third party" to provide packet content and call-identifying information on behalf of rural telephone companies to law enforcement. As they understand it, a "trusted third party" would be a service bureau with a system that would have access to packet networks and that would manage the intercept process for multiple carriers.

The Commission has indicated that use of a "trusted third party" approach would not relieve carriers of their obligation to comply with CALEA. NPRM, at par. 69. Hence, the Coalition needs to explore further how mediation devices and/or external systems would work, how effectively "trusted third parties" could monitor the packet networks of multiple carriers, and what are the risks of CALEA and privacy violations. The Coalition is very interested in the features, capabilities and cost of the hardware and/or software used by "trusted third parties" to monitor packet networks from remote locations, and wonder why such hardware and/or software does not appear to be available to implement CALEA on individual packet networks.

The Coalition recognizes that there may be economies of scale from the use of surveillance equipment to monitor multiple packet networks. On the other hand, it needs to explore the nature and cost of the connections necessary to allow a "trusted third party" to monitor specific rural networks from a remote location, extract content and call-identifying information from packets in response to surveillance orders, and deliver the appropriate information to law enforcement. For rural telephone companies that receive infrequent surveillance requests, these costs may or may not be economically reasonable and feasible.

Conclusion

Rural telephone companies have largely complied with circuit-switched CALEA capability requirements, and are ready and willing to comply with packet-mode CALEA capability requirements once specific and affordable solutions become available from vendors. However, until such time as rural carriers have a practicable means to comply with CALEA, elimination of CALEA Section 107(c) extensions and restriction of CALEA Section 109(b) waivers, as well as establishment of a separate Commission enforcement program, will discourage or effectively prohibit rural deployment of packet-mode facilities and services. If the Commission and the FBI want to accelerate packet-mode CALEA deployment in an effective and equitable manner, they should employ CALEA Section 106 to pressure manufacturers directly to provide timely and affordable CALEA solutions.

Respectfully submitted,
COALITION FOR REASONABLE RURAL BROADBAND CALEA COMPLIANCE

By Gerard J. Duffy

Gerard J. Duffy

Its Attorney

Blooston, Mordkofsky, Dickens, Duffy & Prendergast
2120 L Street, NW (Suite 300)
Washington, DC 20037
Telephone: (202) 659-0830
Facsimile: (202) 828-5568

Dated: November 8, 2004

EXHIBIT A

CISCO SYSTEMS

November 17, 2003

Thank you for your November 14, 2003 inquiry about the support of CALEA functionality for the Cisco products in your client's networks.

Cisco has been developing and testing the ability to intercept IP packets based on source/destination IP address on several of its product platforms, including the 72xx, 75xx, 100xx, 366x. These products must be utilized in conjunction with third party mediation device equipment in order to effect the interception of IP traffic. In addition, your client's ability to effectively conduct the interception of IP traffic will depend on the specific configuration of your network and service they are providing to their customers. A Cisco account manager can provide you more specific information based on your network configuration and service.

Notwithstanding the foregoing, Cisco makes no representations or warranties as to whether or not the platforms listed above will permit your client's compliance with their "packet-mode" CALEA requirements. We recommend that they consult their own legal counsel to determine their specific obligations pursuant to this Act. They may also want to consider contacting a third party mediation device vendor, such as Verint or SS8, regarding the possibility of purchasing alternative "packet-mode" CALEA functionalities compatible with the listed device(s) and or system(s) that they have purchased from our company. Cisco also has identified two companies, VeriSign and Fiducianet, that are CALEA service bureaus. These companies offer various services to assist Service Providers in complying with CALEA.

If you would like additional information regarding Cisco's CALEA strategy, including product release schedules, please contact a Cisco Account Manager.

Sincerely,

Jason Yoder
Sr. Manager, Legal Business Services & Regulatory Affairs
Cisco Systems, Inc.

IP Telephone: 408 526 7045
Email: regaffairs@cisco.com Subject: Lawful Intercept Inquiry

EXHIBIT B

Redback NETWORKS

Redback Networks Inc.
300 Holger Way
San Jose, CA 95134

January 30, 2004~~January 29, 2004~~

Thank you for informing Redback Networks of your goals to fulfill packet mode communications requirements associated with the Communications Assistance for Law Enforcement Act ("CALEA"). Redback has an interest in understanding the long-term requirements for lawful interception of subscriber data. The purpose of this letter is to provide a response to inquiries that you have made with respect to compliance of Redback products to CALEA, in particular section 107(c) regarding packet-mode communications.

A mounting challenge for service providers is to find cost-effective solutions to respond to the exponentially increasing number of subpoenas for data with respect to individual subscriber sessions. As an innovative leader in IP-based technology, Redback is a vendor that is currently developing/investigating cost-effective near-term, and, in some cases, extensible long-term lawful-intercept solutions.

With respect to the full compliance to CALEA for packet mode communications, our view is that the action now rests with the U.S. Federal Communications Commission to provide clear direction and regulations regarding CALEA section 107(c) packet mode petitions. At this early stage of packet mode CALEA requirements, it appears that full CALEA compliance will involve a still-to-be-defined combination of service provider specific infrastructure and network equipment vendor solutions tailored to that infrastructure. We continue to monitor progress in this area, and look forward to the results.

As the CALEA section 107(c) packet mode goals evolve into solid standards, Redback is committed to working with our service provider customer Pymatuning Telephone Company, in a responsive manner, to enable CALEA-compliant broadband networks. The establishment of clear standards will also allow Redback to determine whether and when given product lines will become CALEA compliant. It will also help to drive discussions regarding the status of testing and installation of the equipment. At the present time, these discussions have yet to take place.

Currently, all of Redback SmartEdge and SMS series hardware is manufactured by Jabil Circuit Inc., pursuant to Redback's specifications. This contract manufacturer is one of the best in the industry and currently manufactures equipment for many leading product vendors in addition to Redback Networks.

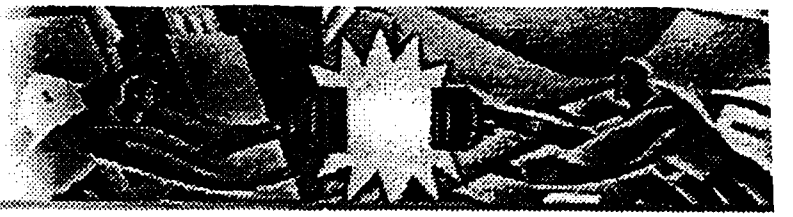
All information contained in this letter is presented without representations or warranties of any kind, whether express or implied, and Redback makes no other legal commitments herein. Redback shall not be held liable for damages of any kind resulting from the furnishing or use of this document.

Sincerely,

James Glover
Product Manager
Redback Networks Inc.

EXHIBIT C

AFC
ADVANCED FIBRE COMMUNICATIONS



Compliance of Advanced Fibre Communications, Inc. ("AFC") Products with the Communication Assistance for Law Enforcement Act, P.L. No. 103-414

AFC would like to inform you as to whether the telecommunications equipment sold to you by AFC is in compliance with the terms of the federal Communication Assistance for Law Enforcement Act, P.L. No. 103-414 ("CALEA") as required by the Federal Communications Commission ("FCC").

Please be advised that the AFC AccessMAX™ and other AFC telecommunications equipment does not provide such capability in compliance with CALEA. Currently, it remains unclear as to whether the Act is intended to apply to digital loop carrier equipment such as AFC's AccessMAX and there is significant support for the position that the Act applies only to switches. In the absence of clear, definitive guidelines from the FCC, AFC has no current plans to provide this capability.

It is possible that various customers of AFC utilize the AccessMAX products to carry Voice over DSL from non-AFC products. The AccessMAX is transparent to these transmissions. Any customer utilizing such a configuration should contact their CPE and Gateway partners for CALEA information.

AFC supports all governmental requirements for Access Equipment. We look forward to supporting our customers in doing so as well. If you should require additional information about AFC products and our compliance with CALEA, please contact your AFC representative.

PARADYNE™

"Paradyne does not believe that its DSL equipment is currently subject to the requirements set forth in the Communications Assistance for Law enforcement Act of 1994 as it is not voice equipment. The J-STD-025A specifies capabilities that may not be required. Further, Standards bodies have been reluctant to advance the J-STD-025A to standard status. It is not clear which direction this may take, so it is our plan to wait until such time that the FCC and/or Federal Court clarifies the issue."

Please note that the ability to "tap" into the communication line to intercept voice traffic is possible, but this would be under the control of the carrier who is managing the traffic and not something that we would or could independently provide.

NET TO NET™
TECHNOLOGIES

November 4, 2003

Re: CALEA Compliance

Attachment: Net to Net CALEA Compliance

To Whom It May Concern:

We, Net to Net Technologies, hereby declare that our products comply with all applicable requirements of the US Communications Assistance for Law Enforcement Act (CALEA).

This declaration is based upon a technical review of the Act (47 USC §1001 – 1010) and our interpretation as detailed in the attachment. This declaration is made solely with the intention of allowing telecommunications carriers to meet their obligations pursuant to said legislation and is true and accurate to the best of our knowledge.

Kenneth J Latimer, Jr.
Chairman and CEO

112 CORPORATE DRIVE, SUITE 1 • PEASE INTERNATIONAL TRADEPORT • PORTSMOUTH, NH 03801
TEL: (603) 427-0600 • FAX: (603) 422-0610
www.nettonettech.com

Net To Net CALEA Compliance

After reviewing the Communications Assistance for Law Enforcement Act (47 USC 1001 – 1010), I have concluded that our products comply with the requirements to the extent that it is possible.

Under CALEA, telecommunications carriers[1] must ensure that their equipment and services, which allow a customer to originate or terminate communications, are capable of the following:

1. Enabling the government to intercept all wire and electronic communications to or from a subscriber;
2. Enabling the government to access call-identifying information;
3. Delivering intercepted communications and call-identifying information to the government; and,
4. Facilitating access to communications interceptions and call-identifying information unobtrusively and with a minimum of interference to service.

Only Items 1 and 2 above can be applied to the hardware. Items 3 and 4 apply specifically to the carrier and their cooperation with the government.

For Net To Net products in a carrier's central office, there are two general categories of upstream communications: data transfer or voice communications (which has been split out of the data stream).

Data Transfer:
If required, the carrier should have no difficulty providing access to the data communications since they own the network to which it is connected. This access should be provided "upstream" of our equipment at the router.

Voice Communications:
Beyond our unit, Voice is split off of the data stream and, like other calls in a CO, is delivered to a phone switch for call routing. If a carrier has the ability to provide access and call-identifying information for calls through the switch, then calls coming through our products to the switch shouldn't be any different. In other words, all access and identifying information can be provided around our unit and not via our unit.

In my investigation into CALEA, I didn't come across any technical standards that we could use to prove compliance that would specifically apply to our products.

---

[1] The term "telecommunications carrier" (a) means an entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire; and (b) includes an entity engaged in providing wire or electronic communication switching or transmission service to the extent that such service is a replacement for a substantial portion of the local telephone exchange service; but (c) does not include entities insofar as they are engaged in providing information services.

To Whom It May Concern,

This letter clarifies how the Avidia system relates to the terms of the Communication Assistance Law Enforcement Act (CALEA).

The Avidia system operates as an access transport device on the edge of the network. The support required by CALEA is provided by the voice switches in the Central Offices of the PSTN and, when applicable, by the Digital Loop Carrier (DLC). The Avidia system is not a voice switch it is an access device. The Avidia system provides inflow/outflow of information into/out of a provider's network. The Avidia system may share the same copper loops with services referred to as Plain Old Telephone Service - POTS, however, when installed and operated as a transport device it shall have no impact on the POTS services. Secondly, the end points of any virtual connection through the Avidia system are network-to-network or network-to-user, never user-to-user. There is no Avidia system application where users transfer information between each other without first going through an upstream device such as a router or data switch. These upstream devices, routers or data switches, provide the required CALEA support in the same way with or without the Avidia system in the network.

ADC DSL System Inc., therefore, declares that the Avidia system (1) is exempt from providing the support defined by CALEA, and (2) shall not adversely affect the support required by CALEA in the network.

Hien Nguyen
Product Application Manager
Avidia Business Unit
ADC DSL System, Inc.