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

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

To: The Commission

COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Telecommunications Industry Association
Matthew J. Flanigan, President
Grant E. Seiffert, Vice President,
External Affairs and Global Policy
Derek R. Khlopin, Director, Law and
Public Policy
2500 Wilson Boulevard, Suite 300
Arlington, VA 22201
Tel: (703) 907-7700
Fax: (703) 907-7727

November 8, 2004

Table of Contents

Page

SUMMARY i

I. Introduction 1

II. Enforcement of CALEA Is the Responsibility of the Federal Courts 4

III. The Commission Must Adopt Reasonable Deadlines for CALEA Compliance 7

IV. The Commission Should Reaffirm the Central Role of the Standards Process in CALEA Compliance 9

- A. TIA and the Standards Process 10
- B. The Commission Should Abandon the Suggestion that Standards Development be Limited to ANSI-Recognized Organizations 12
- C. The Commission Does Not Have Grounds for Finding Existing Standards Deficient 13

V. Trusted Third Party 18

VI. Cost Recovery 20

VII. Conclusion 24

SUMMARY

CALEA requires the Commission to balance law enforcement's needs for effective surveillance capabilities against the risks of over-regulating and stifling innovation. In CALEA, Congress established limited wiretap performance requirements and gave a lead implementation role to the telecommunications industry. The Telecommunications Industry Association ("TIA") has played a key role in developing CALEA standards, including standards for packet-mode communications.

TIA supports the Commission's review of CALEA implementation for packet-mode services in this Notice of Proposed Rulemaking ("NPRM"). In its NPRM, however, the Commission proposes new rules that would change the scope of industry's responsibilities in a manner not supported by CALEA.

First, CALEA places enforcement in the hands of the federal courts. This scheme has not failed; to the contrary, law enforcement has never even tried to use it. There is no statutory basis for the Commission to adopt its own, new enforcement regime for CALEA, particularly one that ignores the statutory defenses to CALEA enforcement. Such a regime would have a substantial adverse effect on technology innovation in the United States. (Section II)

Second, implementation of the major new rules proposed in the NPRM must be coupled with reasonable compliance deadlines. The Commission should require "substantial compliance" – *i.e.*, the ability to deliver the content of covered communications in a manner that they can be identified – within 18 months from issuance of a final rule. Thereafter, any disputes over call-identifying information ("CII") should be handled via the statutory processes of Section 107(b) deficiency petitions and Section 108 enforcement proceedings. (Section III)

Third, industry standards are central to CALEA implementation. The development of the J-STD-025 series of standards by TIA illustrates the potential of the standards process but also shows the pitfalls if law enforcement tries to control that process. The Commission should reaffirm the leading role of industry in the standards process. Although TIA is an ANSI-accredited standards body, it opposes any Commission ruling that would go beyond CALEA to require that standards be issued only by ANSI-accredited organizations.

It is premature for the Commission to consider whether existing packet-mode standards are "deficient" because law enforcement has not identified any specific deficiencies in current standards. Again, CALEA provides a carefully constructed statutory remedy for law enforcement – one that has not been invoked. The Commission should not create a non-statutory shortcut that would disturb the balance established by CALEA. If the deficiency process is followed and deficiencies are identified, any rules that the Commission develops for packet-mode compliance capabilities must take account of the technical characteristics of packet-mode services. (Section IV)

Fourth, "trusted third party" ("TTP") solutions (including solutions funded by law enforcement) offer a promising option for CALEA compliance. In order to avoid impeding the CALEA standards process and giving control of CALEA compliance to law enforcement, however, TTP solutions should not have any special regulatory status. (Section V)

Finally, the Commission has no authority to eliminate the statutory right of carriers to claim reimbursement for CALEA-related intercept costs under Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"). Title III embodies a strong public policy to spread intercept costs (including CALEA costs) – which relate to providing protection from crime and terrorism – across the general public. (Section VI)

These comments are submitted by the Telecommunications Industry Association ("TIA"), a national trade association of 700 small, medium, and large companies that provide communications and information technology products, materials, systems, distribution services, and professional services in the United States and around the world. In addition to representing its members on global policy maters, TIA is accredited by the American National Standards Institute ("ANSI") to develop industry standards.

I. INTRODUCTION

TIA believes strongly that law enforcement must have effective capabilities to conduct lawful surveillance of communications in order to fight crime and terrorism. But in furthering this goal, the Commission must avoid the risks of over-regulating and stifling innovation. Congress recognized this need for balance ten years ago[1] when it passed the Communications Assistance for Law Enforcement Act ("CALEA").[2]

In crafting CALEA, Congress rejected the idea that the federal government should design or even have veto power over new technologies.[3] Instead, Congress established limited performance requirements for wiretap access that apply to a limited portion of the telecommunications industry.[4] CALEA left a great deal of room for innovation and initiative.

---

[1] H.R. Rep. No. 103-827, 1994 U.S.C.C.A.N. 3489, 3493 (1994) ("*Legislative History*") (noting that CALEA balances "three key policies: (1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies.").

[2] Pub. L. 103-414, 108 Stat. 4279 (1994) (codified, as amended, at 18 U.S.C. § 2522 and 47 U.S.C. §§ 229, 1001-1010).

[3] *Id.* at 3499.

[4] *Id.* at 3498.

Importantly, it gave industry the power and freedom to decide how to meet the wiretap requirements: Section 103(b) plainly states that a law enforcement agency may not "require any specific design of equipment, facilities, services, features, or system configurations," nor may a law enforcement agency "prohibit the adoption of any equipment, facility, service, or feature by any provider of a wire or electronic communication service."[5]

Further, Congress gave industry the power to determine how best to comply with CALEA. CALEA's safe harbor provision states that providers are deemed to be in compliance with CALEA if they comply with "publicly available technical requirements or standards adopted by an industry association or standard-setting organization."[6] In the alternative, providers are free to develop their own CALEA compliance solutions if they choose not to rely on an industry standard CALEA solution.[7]

Thus, CALEA allows telecommunications technologies to be deployed freely without government interference – even if they do not have a perfect CALEA wiretap solution. If a carrier deploys an imperfect CALEA solution, then CALEA gives law enforcement a remedy in the courts. And the statute allows carriers to defend themselves against such an enforcement action by showing that full wiretap capability was not reasonably achievable in its system or by showing that law enforcement could get the same information by other means.[8]

TIA rose to CALEA's challenge and has led standards-development efforts ever since CALEA's passage. Working closely with law enforcement, TIA, its member companies, and

---

[5] 47 U.S.C. § 1002(b)(1).

[6] *Id.* at § 1006(a)(2).

[7] *Id.* at § 1006(a)(3).

[8] *Id.* at § 1007.

others involved in TIA's standards programs have defined intercept capabilities for both circuit-switched technologies and a variety of packet-mode technologies, including Voice over IP ("VoIP") and broadband Internet. And TIA remains committed to working with law enforcement and the Commission to ensure standardized intercept capabilities for existing and next generation communications technologies. Jointly with Committee T1 (which is sponsored by the Alliance for Telecommunications Industry Solutions, or "ATIS"), TIA has issued several versions of the leading J-STD-025 CALEA compliance standard, including the recent J-STD-025B revision covering several specific packet-mode services. In fact, TIA member companies have gone well beyond what CALEA requires. For example, many companies that manufacture cable and Internet telephony hardware have already voluntarily built in intercept capabilities, despite uncertainty about whether CALEA applies to those services.

TIA supports the Commission's review of CALEA implementation for packet-mode services in this Notice of Proposed Rulemaking ("NPRM"). However, in several respects, the NPRM proposes new rules that would dramatically change the scope of industry's responsibilities – and the Commission's role in enforcing those responsibilities – in a manner not supported by CALEA. Several issues raised by the NPRM are of particular interest to TIA and its members.

First, there is simply no statutory basis for an entirely new CALEA enforcement regime.

Second, implementation of the significant new rules proposed in the NPRM must be coupled with reasonable compliance deadlines.

Third, the leading role of industry standards in the CALEA implementation process should be reaffirmed.

Fourth, while "trusted third party" solutions offer a promising option for CALEA compliance, such solutions should not have any special regulatory status.

Finally, there is no basis for elimination of the statutory right of carriers to claim reimbursement for intercept costs (including CALEA costs) under Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III").[9]

II. ENFORCEMENT OF CALEA IS THE RESPONSIBILITY OF THE FEDERAL COURTS

The Commission suggests in the NPRM that under Section 229(a) of the Communications Act, it may have general authority to construct an enforcement scheme for CALEA.[10] Implementation of this proposal would be an end-run around the enforcement limits established in CALEA, which give carefully circumscribed enforcement power to the federal courts. In particular, there is no basis for the Commission to turn the requirements of Section 103 of CALEA into Commission rules, as proposed in the NPRM.[11]

Although CALEA confers a number of specific powers upon the Commission, enforcement is not one of them. The Supreme Court has stated that "it is an elemental canon of statutory construction that where a statute expressly provides a particular remedy or remedies, a court must be chary of reading others into it."[12] The Commission's argument under Section 229(a) of the Communications Act suggests that the Commission believes it has general power to

---

[9] Pub. L. 90-351, 82 Stat. 212 (1968) (codified, as amended, at 18 U.S.C. §§ 2510 *et seq*.).

[10] *In re Communications Assistance for Law Enforcement Act and Broadband Access and Services*, Notice of Proposed Rulemaking and Declaratory Ruling, FCC 04-187, ET Dkt. No. 04-295, RM-10865, at ¶ 114 (rel. Aug. 9, 2004) ("*CALEA NPRM*").

[11] *Id.* at ¶ 115.

[12] *Transamerica Mortgage Advisors, Inc. v. Lewis*, 444 U.S. 11, 19 (1979). *See also*, *American Bus Ass'n v. Slater*, 231 F.3d 1, 5 (D.C. Cir. 2000) (same).

take whatever action it wishes to enforce CALEA, regardless of the statutory language. There is no support for this position. Indeed, in recent cases under the Telecommunications Act of 1996, the federal courts have made quite clear that the Commission must take care to follow the statutory scheme set forth by Congress.[13]

Furthermore, the Commission's enforcement proposals in the NPRM[14] simply ignore the statutory defenses specified in Section 108 of CALEA – *i.e.*, that a federal court may take enforcement action under CALEA only if it finds:

> that (1) alternative technologies or capabilities or the facilities of another carrier are not reasonably available to law enforcement . . . and (2) compliance with [CALEA's requirements] is reasonably achievable through the application of available technology to the equipment, facility, or service at issue or would have been reasonably achievable if timely action had been taken.[15]

CALEA requires proof in court on these points before an innovator faces an obligation to design wiretap capabilities into a new product. In contrast, an enforcement scheme like the one envisioned in the NPRM entirely shifts the regulatory balance, imposing far greater pressures for manufacturers to undertake the costs of implementing a CALEA solution before determining whether the new technology will be viable or even bringing it to market. The specter of such a requirement (for example, the prospect of immediate cease-and-desist orders and/or fines before wiretap orders are served) would have a significant chilling effect on all but the most confident innovators.

---

[13] *See United States Telecom Ass'n v. FCC*, 359 F.3d 554 (D.C. Cir. 2004) ("*USTA II*"), *cert. denied sub nom*, *WorldCom, Inc. v. United States Telecom Ass'n*, 538 U.S. 940; *United States Telecom Ass'n v. FCC*, 290 F.3d 415 (D.C. Cir. 2002) ("*USTA I*").

[14] *CALEA NPRM* at ¶¶ 114-116.

[15] 47 U.S.C. § 1007(a). Further, Congress intended to limit the court's authority to issue enforcement orders. "[T]he court must find that law enforcement is seeking to conduct its interception at the best, or most reasonable, place for such interception" and that compliance is reasonably achievable. *Legislative History* at 3508.

TIA recognizes the importance of wiretap capabilities for technologies that are in fact subject to CALEA. But the obligation to introduce such capabilities exists within a carefully crafted statutory framework that includes court enforcement under defined standards. Although the NPRM properly concludes that "Congress did not intend that manufacturers or providers would be required to obtain advance clearance from the government before deploying a technology or service that is not subject to CALEA,"[16] the proposed enforcement scheme has the effect of introducing very similar restraints on innovation. Specifically, immediate introduction of CALEA-compliance capabilities as part of a new technology involves entirely different economic and practical considerations than introduction of such capabilities for mature technologies. It is precisely such considerations that are addressed by the above statutory defenses under the enforcement framework mandated by CALEA.

For example, suppose a manufacturer of a mobile gaming program wants to enable players to be able to talk to each other – perhaps to taunt opponents or to coordinate with team members – and builds in rough voice functionality. The manufacturer will not implement a CALEA solution if it doesn't anticipate that the voice functionality will be used in a manner that will satisfy the "substantial replacement" test or otherwise implicate CALEA requirements. However, if such unanticipated usage does develop, the manufacturer will only be required to add CALEA functionality if law enforcement can prove that (a) alternative wiretap technologies or capabilities are not reasonably available and (b) the manufacturer's compliance is reasonably achievable. But if the Commission's proposed regulatory scheme is implemented, then the manufacturer may never even bring to fruition its idea for voice communications for its mobile gaming function, because the development cost of adding CALEA capabilities (or the cost of

[16] *CALEA NPRM* at ¶ 61.

obtaining a ruling from the Commission that the capabilities are not required) may outweigh the perceived market opportunities for the product.

The likely effect of such CALEA compliance and enforcement burdens will be to drive development and testing of new technologies abroad, to the detriment of U.S.-based industry, U.S. technical personnel, and U.S. consumers. Many companies – including the numerous TIA members who are based in other countries – choose the United States for development of technology because of its strong culture of innovation and availability of some of the world's most qualified technical personnel in places like Silicon Valley. But the strong U.S. position is not immune from threat. On the contrary, other nations have already embraced broadband with far more enthusiasm than the United States, which no longer ranks even among the top ten nations in the world in terms of broadband penetration.[17] And numerous governments around the world are providing incentives for technology research and development in their countries.

In sum, the approach to CALEA enforcement proposed in the NPRM is unsupported by the text of the statute and would run counter to the statutory goal of "avoid[ing] impeding the development of new communications services and technologies,"[18] to the particular detriment of U.S.-based technology companies. The Commission should simply leave CALEA enforcement to the federal courts, as Congress decided.

III. THE COMMISSION MUST ADOPT REASONABLE DEADLINES FOR CALEA COMPLIANCE

If the Commission moves ahead with its tentative conclusions to regulate many broadband access and VoIP services under CALEA, it must impose reasonable deadlines for

---

[17] Thomas W. Hazlett, et al., *Sending the Right Signals: Promoting Competition Through Telecommunications Reform*, A Report to the U.S. Chamber of Commerce (Sept. 22, 2004) at 44.

[18] *Legislative History* at 3493.

these major new obligations on Internet and VoIP service providers. Such deadlines must take account of the industry standards process, including the time required for manufacturers to work with law enforcement to develop CALEA solutions that balance the needs of industry and law enforcement (see section IV below). Compliance deadlines also must provide time for equipment manufacturers to design and develop CALEA solutions sufficiently in advance of the compliance deadline to allow the solutions to be implemented in products being deployed in the market.

TIA suggests that companies with currently existing technologies that would be newly subject to CALEA should have at least 18 months from the date on which any final rule is issued in this proceeding to achieve substantial compliance with those rules. For the purposes of determining whether a company has met its deadline, "substantial compliance" would be defined as the achievement of sufficient wiretap capability so that criminals could not use the service without the content of their communications being subject to interception. TIA acknowledges that such a standard might leave room for argument about the particular types of call-identifying information ("CII") that must be provided, but the standard would at least ensure that individuals who are properly the subject of a wiretap order would not be able to hide their communications from law enforcement.[19]

After the 18-month substantial compliance deadline, more detailed requirements for CII would continue to be developed as provided by CALEA. That is, CII requirements would be established in the industry standards process under Section 107(a) of CALEA, subject to the rights of law enforcement to allege that industry standards are deficient under Section 107(b) or to seek enforcement under Section 108. Once the deadline for "substantial compliance" passes,

[19] This would be subject to the existing CALEA exception for user-provided encryption. *See* 47 U.S.C. § 1002(b)(3).

law enforcement would be free to seek such statutory remedies with respect to the details of compliance where it disagrees with industry solutions. But TIA is hopeful that proper functioning of the industry standards process will render such actions unnecessary and will provide standards that both meet the requirements of CALEA and satisfy the intercept needs of law enforcement.

For any new technologies that in the future become subject to CALEA under any "substantial replacement" test the Commission adopts, TIA suggests measuring the deadline for "substantial compliance" from the date on which the product was deemed to be a "substantial replacement." This definition would capture the date on which the technology is actually in widespread use, rather than the date on which the product was first deployed. This approach would provide an appropriate amount of time for the CALEA standards process to function (and would address the innovation issues discussed in section II above).

IV. THE COMMISSION SHOULD REAFFIRM THE CENTRAL ROLE OF THE STANDARDS PROCESS IN CALEA COMPLIANCE

In enacting CALEA, Congress recognized that industry-led standards development efforts are critical to the cost-effective and successful implementation of CALEA. Now, as part of its effort to expand CALEA to broadband access providers and VoIP providers, the Commission should reaffirm the central role of the standards process and should reject any attempt by law enforcement to control that process.

Section 107(a) of CALEA provides that a carrier complying with a CALEA standard "*shall* be found to be in compliance" with CALEA's intercept capability requirements.[20] As the D.C. Circuit explained:

[20] *Id.* at § 1006(a)(2) (emphasis added).

> To ensure efficient and uniform implementation of the Act's surveillance assistance requirements without stifling technological innovation, CALEA permits the telecommunications industry, in consultation with law enforcement agencies, regulators, and consumers, to develop its own technical standards for meeting the required surveillance capabilities.[21]

Congress rejected an approach that was under consideration in early drafts of CALEA and would have allowed law enforcement to dictate CALEA standards. Instead, it specifically prohibited law enforcement from "requir[ing] any specific design of equipment, facilities, services, features, or system configurations."[22] The role of law enforcement is limited to one of "consultation."[23]

A. TIA and the Standards Process

TIA, its member companies, and other participants in TIA's standards activities have worked diligently for nearly a decade to adopt and improve CALEA standards that provide law enforcement intercept capabilities consistent with CALEA's statutory requirements.[24] TIA's core CALEA standards project has been the J-STD-025 series of standards, which TIA has pursued jointly with ATIS Committee T1 since shortly after CALEA was enacted in 1994. This series includes the original J-STD-025, covering circuit-mode services in detail and (the then-much newer) packet-mode services in lesser detail; J-STD-025A, which adds much of the FBI "punch list" for circuit-mode services; J-STD-025B, adding detailed surveillance capabilities for the three packet-mode platforms: cdma2000® not implementing call management server

---

[21] *United States Telecom Ass'n v. FCC*, 227 F.3d 450, 455 (D.C. Cir. 2000).

[22] 47 U.S.C. § 1002(b)(1)(A). *See also*, *Legislative History* at 3499 ("The bill expressly provides that law enforcement may not dictate system design features and may not bar introduction of new features and technologies. ... This is the exact opposite of the original versions of the legislation, which would have barred introduction of services or features that could not be tapped.").

[23] 47 U.S.C. § 1006(a)(1).

[24] Reply Comments of the Telecommunications Industry Association, Declaration of Terri L. Brooks, ET Dkt. No. 04-295, RM-10865 (filed Apr. 27, 2004) ("*Brooks Declaration*").

("CMS") functionality, UMTS/GPRS,[25] and a voice-over-packet standard for wireline networks. TIA is continuing to develop surveillance standards for cdma2000® IMS (CMS services) under the project number SP-3-1099.

The J-STD-025 process illustrates both the potential and the pitfalls of the standards process. For example, J-STD-025A, though now accepted by all, was delayed by law enforcement because of the refusal of TIA and T1 to adopt the entire FBI "punch list." Initial law enforcement tactics against J-STD-025 included an effort to de-certify TIA as a standard-setting organization[26] and an effort to block adoption of the standard by soliciting numerous identical "no" votes from local law enforcement agencies that had not otherwise participated in the standards process.[27] In the end, when these extra-statutory tactics failed, law enforcement pursued the statutory route of a deficiency petition under Section 107(b) of CALEA, with the result that some "punch list" capabilities were adopted and some were not.

Again, when J-STD-025B was in development, law enforcement attempted to assert control over the standards process despite the absence of a statutory basis for doing so. Indeed, the FBI took the position that TIA lacked authority to consider the legal requirements of CALEA in the standards process.[28] The result was that J-STD-025B was adopted without the agreement of law enforcement. It became a valid CALEA safe harbor standard in January 2004. If law enforcement considers some portion of that standard deficient, it should follow the statutory

---

[25] "UMTS/GPRS" stands for Universal Mobile Telecommunications System/General Packet Radio Service.

[26] *Brooks Declaration* at 6.

[27] *Id.* at 5-6.

[28] *Id.* at 13, Attachment C (Letter from Leslie M. Szwajkowski, FBI, to Terri Brooks, TIA (Feb. 28, 2003)).

route of a Section 107(b) deficiency petition. This process will produce an answer whose legal status is unchallenged.

But this time, law enforcement has opted not to follow that process. Instead, it has mounted a wholesale challenge to the statutory framework of CALEA by filing the petition that led to this NPRM. The Commission should reject the effort to create extra-statutory "solutions" and procedures. In the end, they are unlikely to prove faster if each party genuinely believes that its view of the law is correct, and the Commission will find itself thrust into the middle of extensive technical disputes that are currently refined and sharpened in the standards process before any deficiency procedure is launched.

B. The Commission Should Abandon the Suggestion that Standards Development be Limited to ANSI-Recognized Organizations

Although TIA is an ANSI-accredited[29] standards-setting organization, its members strongly urge the Commission to abandon the suggestion that the development of standards could be limited to ANSI-accredited organizations.[30]

Most important, the language of CALEA contains no such limitation. To the contrary, CALEA provides that safe harbor standards may be "adopted by an industry association or standard-setting organization"[31] – *i.e.*, not only is there no accreditation requirement, but the statute is explicit in stating that an industry association that is not "standard-setting organization" may issue CALEA standards. And, in fact, the great majority of all the CALEA standards that have been adopted were developed outside the ANSI process. These include (1) the dispatch

[29] ANSI (the American National Standards Institute) is a non-profit organization that administers and coordinates the U.S. standards and conformity assessment system. *See* http://www.ansi.org (last visited Nov. 8, 2004).

[30] *CALEA NPRM* at ¶ 80.

[31] 47 U.S.C. § 1006(a)(2).

standard developed by the American Mobile Telecommunications Association in 1999, and updated in 2004; (2) the CableLabs® standard developed in 1999 and updated twice since then at the request of law enforcement; (3) the paging standard developed by PCIA in 1998; and (4) several IETF RFCs developed primarily by Cisco. Thus, an ANSI-accreditation requirement would strike down several existing standards that have never been challenged as deficient, even though they were adopted at about the same time as the standards issued by the ANSI-accredited TIA.

By limiting standards development to ANSI-accredited organizations, the Commission would also encourage improper law enforcement tactics, such as the efforts discussed above, to challenge TIA's ANSI accreditation and to manipulate the ANSI consensus requirement by using local law enforcement votes to oppose standards that enjoy consensus support from industry. This likely would have the effects of magnifying the law enforcement role in the standards process beyond its statutory role of "consultation" and would increase disruption and delay of the standards process.

C. The Commission Does Not Have Grounds for Finding Existing Standards Deficient

The Commission seeks comment on whether existing packet-mode standards developed by organizations such as TIA and CableLabs® are deficient.[32] It will be most appropriate to address particular claims of deficiency in the reply comments round, if and when law enforcement and/or other commenters have identified particular deficiencies in standards. But a few initial comments may be appropriate concerning issues that have already been raised by law enforcement informally.

[32] *CALEA NPRM* at ¶ 80.

First, as the Commission recognizes, extraction of CII presents particular difficulties in the packet-mode environment:

> Call-identifying information may be found within several encapsulated layers of protocols. … As the packet makes its way through the network of the broadband access service and Internet service providers, these providers' equipment generally do not examine or process information in the layers used to control packet-mode services such as VoIP, and in fact operate at layers below the ones that carry control information for broadband access services. As a result, the broadband access service and Internet service providers may not be able to easily isolate call-identifying information for VoIP without examining the packet in detail, or in other words, examining the packet content.[33]

TIA agrees with these observations. That is, the Commission must recognize that different CALEA compliance capabilities are appropriate for service providers operating at different layers of packet-mode networks. For carriers handling packets at lower layers, extraction of particular call-identifying information at higher layers may be difficult or impossible.

Second, the Commission has again raised its previous conclusion that "information may not be 'reasonably' available if the information is only accessible by significantly modifying a network"[34] The defensibility of this approach depends upon what the Commission means by "significantly modifying a network." In earlier proceedings, the Commission concluded that CII is "reasonably available" only if it is "present at a carrier's IAP [intercept access point] and can be made available without the carrier being unduly burdened with network modifications."[35] In the NPRM, however, the Commission appears to suggest that CALEA's "reasonably available" language may mean that if a provider *could* access the information without dramatically

---

[33] *Id.* at ¶ 65.

[34] *Id.* at ¶ 67-68

[35] *In re Communications Assistance for Law Enforcement Act*, Third Report and Order, 14 FCC Rcd 16794, 16808 ¶ 28 (1999) ("*Third Report and Order*").

reengineering its system (even if it has no use for the information), then the provider will be required to provide the information to law enforcement – regardless of the costs of doing so.

This is radically inconsistent with CALEA. Cost considerations are fundamental to the structure of CALEA, including for evaluation of deficiency petitions under Section 107(b) and "reasonably achievable" petitions under Section 109(b). Moreover, it would be a nonsensical reading of the statute to suggest that information is "reasonably available" to a carrier (a) even though the information is not used in the carrier's ordinary operations and (b) regardless of the cost of extracting such information.

Likewise, it makes no sense for the Commission to state that in the dialed-digit extraction context "we did not view cost as a factor in whether information is 'reasonably available' … [but rather] that cost concerns were best addressed as part of a section 107(b) analysis."[36] In fact, it is *only* in the context of 107(b) (when industry standards are absent or deficient) that the Commission has authority to prescribe rules on call-identifying information. And, indeed, the Commission in the past has consistently considered cost issues in its analysis of CALEA's requirements.[37]

Third, as the Commission recognizes, "[p]acket technologies are fundamentally different from the circuit-switched technologies that were the primary focus of the Commission's earlier decisions on CALEA."[38] Likewise, CII on packet networks is very different than CII on circuit-switched networks; and the Commission's findings that some kinds of CII are "reasonably

---

[36] *CALEA NPRM* at ¶ 67.

[37] *Third Report and Order* at 16809 (concluding that "[i]n addition to network design considerations, … cost and privacy considerations [are] to be considered in determining whether call-identifying information is 'reasonably available' to an originating carrier.").

[38] *CALEA NPRM* at ¶ 63.

available" on circuit-switched networks cannot control the same inquiry with respect to packet networks.

Fourth, TIA has adopted packet-mode standards (including J-STD-025B) focused on technology platforms, rather than on the services provided over those platforms.[39] The NPRM notes that "a technology platform approach could define a set of network events common to all services and specify call-identifying information that could be extracted without analyzing more of the packet than would otherwise be required to process the packet."[40] TIA believes that this approach is robust and efficient. Because services evolve faster than platforms, a service-focused approach is difficult to implement and susceptible to rapid obsolescence. Again, however, if law enforcement believes that platform-focused TIA standards fail to provide for delivery of particular call-identifying information that is reasonably available under CALEA, it should identify such deficiencies for consideration by the Commission under Section 107(b).

The advantages of an industry-led, platform-based approach to developing intercept standards can be illustrated in the standards currently being developed for wireless IP-based multimedia services. Two nearly identical wireless multimedia "platforms" have been developed over which a variety of multimedia applications can be run (such as voice over packet, push-to-talk, and video). These platforms are IP Multimedia Subsystem ("IMS") and Multi-Media Domain ("MMD"). Instead of developing a separate intercept standard for every conceivable application that could run across the IMS and MMD platforms, TIA and other industry groups (such as 3GPP[41]) have been developing an intercept standard based on the fact that both

---

[39] *Id.* at ¶ 78.

[40] *Id.* (citing *Brooks Declaration* at 11).

[41] "3GPP" stands for 3rd Generation Partnership Project.

platforms use Session Initiation Protocol ("SIP") for signaling and communications-identifying information.[42]

Because SIP is the signaling protocol used for many current and future IMS/MMD applications, such as voice over packet and push-to-talk over cellular, it makes sense to build a lawful intercept standard around SIP. This ensures that law enforcement will be able to get CII for multimedia applications running over those platforms both now and in the future. SIP is also emerging as *the* signaling protocol for multimedia applications in wireline networks. As law enforcement's needs change, they will only have to query the parameters in the SIP signaling message to get the relevant information. Law enforcement will not have to develop a new standard or expand their proprietary intercept protocol. Rather, by sending the SIP message to law enforcement, law enforcement will receive everything that the network operator has in terms of signaling to or from the intercept subject.

Using this SIP-based approach, the 3GPP group issued 3GPP TS 33.108, a lawful intercept standard for the IMS platform[43] that has been widely deployed in Europe since its release 18 months ago. Under this standard, communications-identifying information for IMS is delivered to law enforcement by wrapping each SIP signaling information message in an electronic envelop with the necessary information for law enforcement (case ID, time/date, and system identity) and then sending it directly to law enforcement. This approach has generally

---

[42] SIP was developed by the Internet Engineering Task Force ("IETF"), and is designed to be a part of the overall IETF multimedia data and control architecture, and is globally deployed. SIP is considered to be a flexible solution, simple and easy to implement, better suited to the support of intelligent user devices, and better suited to the implementation of advanced features.

[43] 3GPP TS 33.108 "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Handover interface for Lawful Interception" (Release 5).

worked well in Europe; not one service provider or law enforcement agency has complained that the IMS interception method is ineffective. It has been a win-win result for industry and law enforcement.

But when 3GPP TS 33.108 was balloted by ATIS in the United States as T1.724, it was rejected by law enforcement, which wants industry to extract the SIP information and map it onto a special law enforcement protocol that is likely to vary by multimedia application. This has delayed the completion of this standard and will delay the access of U.S. law enforcement to SIP signaling information in the future by forcing a renegotiation and new standard for every new service built on SIP technology.[44]

V. TRUSTED THIRD PARTY

A "trusted third party" ("TTP") approach has the potential benefit of offering efficient and standardized CALEA compliance solutions. If a few vendors develop workable and cost-effective CALEA solutions, there is no reason to force other manufacturers to develop redundant solutions, particularly if those solutions are not likely to find a market because they are too costly. Furthermore, a TTP funded by law enforcement – or "owned by ... Law Enforcement," as

[44] In addition, a standard is not deficient if it does not contain a standard format for delivery of wiretap information. *CALEA NPRM* at ¶ 84. In its *Third Report and Order*, the Commission rejected a law enforcement proposal for a standardized delivery interface, noting that law enforcement had already conceded that there is no such requirement. 14 FCC Rcd at 16852 ¶ 136 (noting that "[a]s Assistant Attorney General Colgate stated in February 1998, 'a single delivery interface is not mandated by CALEA.'"). The Commission found that nothing in CALEA "would require that the number of interfaces be limited." But the Commission did note that industry may eventually "reach agreement on a relatively limited number of delivery interfaces, which should serve to reduce costs to LEAs," as digital technology evolves. *Id.* Indeed, for example, the format of the CII provided pursuant to the T1.724 standard is exactly the same as that being used to provide wiretap information to law enforcement authorities in Germany, the Netherlands and the United Kingdom.

the NPRM suggests[45] – could facilitate interactions among carriers, manufacturers, and law enforcement, and could play a significant role in relieving burdens on small law enforcement agencies.

But CALEA does not provide any special status or different capability requirements where a compliance solution is provided by a TTP. In particular, the Commission should not conclude that particular CII is "reasonably available" simply because a TTP has announced a willingness to extract it for a price. The Commission should apply the ordinary factors under Section 107(b) of CALEA (including cost considerations) to determine whether TTP-provided capabilities are "reasonably available."

The Commission indicates that there may be a "tension between relying on a trusted third party model and relying on 'safe harbor' standards."[46] But this tension can be entirely eliminated by giving the industry standards process the lead role set out in the statute and by avoiding any special role for TTPs, which are not mentioned at all in CALEA. The standards process, which includes deficiency proceedings before the Commission, will help define the scope of capabilities that TTPs (and other entities) offer by separating CALEA requirements from law enforcement's wish list. If a TTP has developed cost-effective procedures or equipment for meeting CALEA requirements, industry has no reason not to adopt standards that incorporate those procedures and equipment.

A legally favored status, in contrast, would give TTPs the incentive to adopt capabilities beyond those required by CALEA. And TTPs would have the ability to pass the costs of those additional capabilities on to carriers, if cost-effective, non-TTP solutions are forced out of the

---

[45] *CALEA NPRM* at ¶ 75.

[46] *Id.* at ¶ 73.

market by legally favored TTPs. Of course, there is nothing to prevent law enforcement from funding a TTP to develop capabilities beyond those required by CALEA. That is, in effect, what the FBI did in purchasing from switch vendors several intercept features that had been rejected by the Commission and the courts. It is also what the FBI did in building and deploying Carnivore, a device that separates properly intercepted bits from bits that may not be intercepted. But in each case, law enforcement paid for the features law enforcement wanted. TTP offerings *should* play a significant role in CALEA compliance if they offer cost-effective compliance options. But the statute does not favor a TTP solution over an industry-led solution that meets the statutory requirements at lower cost.

VI. COST RECOVERY

In the petition underlying this NPRM, law enforcement asks the Commission to place the entire cost burden of CALEA compliance on industry,[47] and the Commission responds in the NPRM by asking for "comment on the costs that can be included in intercept provisioning costs and the entities that should bear financial responsibility for those costs."[48] In asking for such comment, the Commission has failed to consider the threshold issue of whether it has statutory authority to regulate in this area. It does not.

As the Commission has recognized, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III")[49] explicitly provides that intercept orders are to be issued by a

---

[47] *See* United States Department of Justice, Federal Bureau of Investigation and Drug Enforcement Administration, Joint Petition for Expedited Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance for Law Enforcement Act, RM-10865 (filed Mar. 10, 2004), at 63.

[48] *CALEA NPRM* at ¶ 133.

[49] Pub. L. 90-351, 82 Stat. 212 (1968) (codified, as amended, at 18 U.S.C. §§ 2510 *et seq.*).

"judge of competent jurisdiction"[50] and that "[a]ny provider of wire or electronic communication service, landlord, custodian or other person furnishing such [intercept] facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance."[51] The Commission is not authorized to issue intercept orders, nor to decide how Title III should be construed. In particular, the Commission is given no authority to determine how a judge of competent jurisdiction should determine what constitute "reasonable expenses incurred in providing … facilities or assistance."[52]

In the 35 years since Title III was enacted, the Commission has not regulated intercept cost recovery. This is for good reason: there is no statutory basis for it to do so. Indeed, neither law enforcement nor the Commission suggests a proper statutory basis for such regulation. To the extent that the Commission reads section 229(a) of the Communications Act as a grant of authority to regulate cost recovery, as it does in the context of CALEA enforcement authority, it is equally incorrect. Section 229(a) of the Communications Act permits the Commission to "prescribe such rules as are necessary to implement the requirements of" CALEA[53] – not to rewrite the rules under a statute passed 25 years before CALEA.

Although costs related to CALEA undoubtedly have been part of the "reasonable expenses" recovered by carriers for years, to our knowledge no law enforcement agency has ever

---

[50] *Id.* at § 2518(1).

[51] *Id.* at § 2518(4). In addition, the court issuing a surveillance order generally has authority to order cost recovery for other types of surveillance as well. *Id.* at §§ 2706 (stored electronic communications), § 3124(c) (pen registers, trap/trace devices).

[52] *Id.* at § 2518(4).

[53] 47 U.S.C. § 229(a). Furthermore, the language of section 229(a) authorizing rules to "implement" CALEA is inherently inconsistent with a use of the section as authority for rules addressing matters not covered by the statute.

challenged the inclusion of such costs in the forum provided by Title III. The Commission recognized the reality of this long practice when it noted that:

> carriers can recover at least a portion of their CALEA software and hardware costs by charging to [law enforcement agencies], for each electronic surveillance order authorized by CALEA, a fee that includes recovery of capital costs, as well as recovery of specific costs associated with each order.[54]

When it made this statement, the Commission in no way suggested that it had authority to alter this cost recovery framework under Title III. But if the Commission did have authority to modify Title III, it reached the right conclusion the first time.

Charging CALEA compliance costs to law enforcement, and thus to the public at large, also is good policy. The NPRM notes the "public benefits of CALEA-supported surveillance of criminals and terrorists," and properly asks if CALEA costs should be spread "more equitably … among the general public."[55] In fact, security from crime and terrorism is a classic public good: the benefits accrue to the public at large, the addition of beneficiaries does not diminish the utility of the security, and nobody can be excluded from the benefits (regardless of whether they have paid for them).[56] It is a well-settled economic theory that public goods are provided efficiently only when they are paid for by the public.[57]

Perhaps equally important, the immediate beneficiaries of new CALEA features are law enforcement agencies, who also are important participants in the process of deciding how to implement CALEA. If they can ask for every desired capability and pay none of the costs, the

---

[54] *In re Communications Assistance for Law Enforcement Act*, Order on Remand, 17 FCC Rcd 6896, 6917 ¶ 60 (2002).

[55] *CALEA NPRM* at ¶ 127.

[56] PAUL A. SAMUELSON & WILLIAM D. NORDHAUS, ECONOMICS 36 (16th ed. 1998).

[57] *Id.*

temptation to do so will be irresistible. But if the cost of a gold-plated system finds its way eventually into their budgets, law enforcement agencies may well decide that copper plating will do quite well enough. The incentives of law enforcement where cost is separated from benefit have been all too clear over the years since CALEA was passed, and the Commission certainly should not now magnify these incentives by seeking to eliminate, without statutory authority, recovery of CALEA costs under Title III. Only in matching the beneficiary and the cost will efficient, reasonable decisions be made about how to implement CALEA.

Elimination of Title III cost recovery authority would increase the price, and therefore decrease the availability, of telecommunications services subject to CALEA. The burden would be particularly heavy on providers of broadband access and telephony services, who, for the first time, may now be required to implement CALEA compliance solutions. These effects would run counter to the objective of CALEA to "avoid impeding the development of new communications services and technologies,"[58] as well as to the broader Commission mandate under the Telecommunications Act of 1996 to "encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans … ."[59]

Finally, reversing its original view of Title III would thrust the Commission into numerous additional disputes over whether and how carriers can recover costs for CALEA expenditures. Title III plainly requires recovery for expenses incurred in providing "facilities" as well as "assistance"; and since capital costs are the main expenses associated with providing facilities, it is plain that intercept-related capital costs are recoverable. If the Commission adopts a rule denying CALEA costs under Title III, it would need to decide which capital expenses

---

[58] *Legislative History* at 3493.

[59] 47 U.S.C. § 157nt.

remain recoverable and which are "CALEA-related," non-recoverable expenses. This would be particularly difficult with respect to network equipment (*e.g.*, dual tone multi-frequency detectors) of a kind that was being purchased to assist law enforcement long before CALEA was passed. If the costs of such purchases are non-recoverable, then the rule suggested in the NPRM would effectively amend Title III to prohibit recovery of capital costs relating to the "facilities" used to assist law enforcement. If it is beyond the Commission's power to construe Title III, surely it is beyond the Commission's power to amend it.

VII. CONCLUSION

TIA supports the Commission's goal of encouraging the development of intercept capabilities for new technologies. But the Commission must do so in a manner consistent with the text and legislative history of CALEA. In particular, TIA urges the Commission to take into account the particular implementation concerns set forth above.

Respectfully submitted,

Stewart A. Baker

For Telecommunications Industry Association
Matthew J. Flanigan, President
Grant E. Seiffert, Vice President,
External Affairs and Global Policy
Derek R. Khlopin, Director, Law and
Public Policy

Of Counsel:
Stewart A. Baker
Maury D. Shenk
Emily Hancock
Steptoe & Johnson LLP
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036

November 8, 2004