

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, DC 20554**

In the Matter of	)	
	)	
Petition for Expedited Rulemaking	)	RM No. 11376
to Establish Technical Requirements	)	
and Standards Pursuant to Section 107(b)	)	
of the Communications Assistance for	)	
for Law Enforcement Act	)	

---

**COMMENTS OF AT&T, INC.**

---

Theodore C. Marcus  
Jack Zinman  
Gary L. Phillips  
Paul K. Mancini

AT&T Services, Inc.  
1120 20<sup>th</sup> Street, N.W.  
Suite 1000  
Washington, D.C. 20036  
(202) 457-2044 - telephone  
(202) 457-3073 - facsimile

Its Attorneys

July 25, 2007

## Table of Contents

I.	BACKGROUND.....	2
A.	CALEA.....	2
1.	The Original J-Standard.....	4
2.	J-STD-025-B.....	6
II.	LEGAL STANDARDS FOR DOJ’S PETITION.....	7
III.	DISCUSSION.....	9
A.	“Buffering” ( <i>i.e.</i> , Storage) Is Not Required By CALEA.....	9
B.	“Packet Activity Reporting” Is Burden-Shifting By Another Name.....	12
C.	Disposition of the Present J-STD-025-B Question In Favor of DOJ Should Not Be Automatically Applicable to Other CALEA Standards.....	14
IV.	CONCLUSION.....	16

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

In the Matter of	)	
	)	
Petition for Expedited Rulemaking	)	RM No. 11376
to Establish Technical Requirements	)	
and Standards Pursuant to Section 107(b)	)	
of the Communications Assistance for	)	
Law Enforcement Act	)	

**COMMENTS**

AT&T Inc., on behalf of itself and its affiliates (collectively referred to as “AT&T”), files these comments in response to the Department of Justice’s Petition for Expedited Rulemaking (“Petition”), filed May 15, 2007 in the above-captioned docket.

The Petition asks the Commission to find that the industry standard, J-STD-025-B (also referred to herein as the “J-Standard” or “packet-mode standard”), is deficient for ensuring CALEA compliance for packet-mode communications employing a particular wireless packet technology known as CDMA2000, and to initiate a rulemaking for the establishment of CALEA-compliant rules for law enforcement surveillance involving packet-mode communications using that technology. AT&T, though it does not utilize CDMA2000 in the provision of any of its wireless services, nevertheless believes that DOJ’s Petition substantially lacks merit and should be denied by the Commission. The capabilities that DOJ seeks are not authorized by the CALEA statute. Beyond that, DOJ’s request would impose substantial and unjustified costs that would ultimately have to be borne by ratepayers. Finally, the Commission should reject DOJ’s suggestion that any standards it might ultimately deem appropriate in the present context should automatically become applicable in other CALEA contexts that are not presently before the Commission. Because DOJ has not even alleged, let alone demonstrated, any deficiency in these

other unspecified contexts, the Commission should summarily decline DOJ's invitation to engage in such arbitrary and capricious rulemaking.

## **I. BACKGROUND.**

### **A. CALEA.**

CALEA requires telecommunications carriers to ensure that their networks are technically capable of enabling law enforcement agents, operating under proper legal authority, to intercept individual communications (whether circuit-mode or packet-mode), and obtain certain "call-identifying information" from those intercepts.<sup>1</sup> CALEA section 103 enumerates electronic surveillance assistance capability requirements with which carriers must comply. Carriers must ensure that their equipment, facilities or services used to provide subscribers with the ability to make and complete calls must be capable of: (1) expeditiously isolating a surveillance subject's circuit-mode and packet-mode communications from the communications of others, and enabling law enforcement agents (LEAs), when legally authorized to do so, to intercept such communications; (2) expeditiously isolating call-identifying information associated with such communications and enabling LEAs, when authorized, to access that information, if it is reasonably available to the carrier, at a pre-determined point "in a manner that allows it to be associated with the communication to which it pertains;" (3) delivering the intercepted communications and/or call-identifying information (depending upon the legal authorization provided) to the DOJ in a "format such that they may be transmitted by means of equipment, facilities, or services procured by the DOJ" to designated locations off the carrier's premises; and (4) facilitating the enumerated activities unobtrusively, with minimal service

---

<sup>1</sup> See 47 U.S.C. § 1002; *United States Telecom Association et al. v. F.C.C. et al*, 227 F.3d 450, 453 (D.C. Cir. 2000).

interference, and in a fashion that protects the privacy and security of communications not authorized to be intercepted, and also shields the DOJ's surveillance operations from disclosure.

CALEA does not impose limits on the advancement or evolution of telecommunications technology and services. To the contrary, as the Commission has observed, CALEA only seeks to *preserve* law enforcement's ability to "conduct surveillance effectively and efficiently in the face" of rapidly advancing telecommunications technology while, of course, safeguarding the privacy of individuals not subject to lawfully authorized surveillance.<sup>2</sup>

In order to "ensure efficient and uniform implementation of the Act's surveillance assistance requirements without stifling technological innovation, CALEA permits the telecommunications industry, *in consultation* [but not in tandem] with law enforcement agencies, regulators, and consumers, *to develop its own technical standards* for meeting the required surveillance capabilities."<sup>3</sup> In particular, CALEA section 107 (a) (2) establishes a "safe harbor" based on compliance with industry-developed standards:

A telecommunications carrier *shall* be found to be in compliance with the assistance capability requirements under section 103 . . . if the carrier . . . is in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization . . . to meet the requirements of section 103.<sup>4</sup>

---

<sup>2</sup> *In Re: Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, *Third Report and Order*, 14 FCC Rcd 16794, ¶ 3 (1999) (*Third Report and Order*). See *United States Telecom*, 227 F. 3d at 454. CALEA, thus, does not displace but affirms other requirements of law traditionally applicable to law enforcement's surveillance operations, *e.g.*, warrant requirements for content intercepts, and privacy-driven legal requirements regarding the intercept of call-identifying information through pen registers (which record call identifying information of a subject's outgoing calls) or trap and trace devices (which record call identifying information of a subject's inbound calls).

<sup>3</sup> *United States Telecom Association*, 227 F. 3d at 455 (citing 47 U.S.C. § 1006) (emphases added), and 460 ("Rather than simply delegating power to implement [CALEA] to the Commission, Congress gave the telecommunications industry the first crack at developing standards . . . Congress obviously expected industry to play [a major role] in formulating CALEA standards.").

<sup>4</sup> *Third Report and Order*, 14 FCC Rcd 16794 at ¶ 4.

Thus, although carriers are free to choose independent routes to CALEA compliance,<sup>5</sup> carriers may opt – and many carriers have opted – to rely upon the standard-setting process of accredited organizations to take advantage of the “safe harbor” such standards provide.

### **1. The Original J-Standard.**

The CALEA safe harbor compliance standard at issue in the DOJ’s Petition was originally published jointly by the Telecommunications Industry Association (TIA) and the Alliance for Telecommunications Industry Solutions (ATIS) in December 1997. This standard, declared interim at the time, was the culmination of two years of extensive proceedings during which active, in-depth discussions and negotiations were held with the Federal Bureau of Investigations (FBI). The standard, known as “J-STD-025” or the “J-Standard,” outlined the technical features, specifications, and protocols for carriers in making subscriber communications and call-identifying information available to [LEAs] having appropriate authorization.”<sup>6</sup>

The standard was challenged before the Commission both as over-inclusive and under-inclusive by various parties after publication. The DOJ, specifically, contended that the J-Standard was deficient because it failed to provide for nine capabilities the DOJ deemed “essential.”<sup>7</sup> Others, including the Center for Democracy and Technology and the Electronic

---

<sup>5</sup> *Id.* at n. 7.

<sup>6</sup> *United States Telecom Association*, 227 F. 3d at 455. *See Third Report and Order*, 14 FCC Rcd 16794 at ¶ 5 (The standard, which addressed both circuit-mode communications and packet-mode communications when originally published, “defines services and features required by wireline, cellular, and broadband PCS carriers to support lawfully authorized electronic surveillance, and specifies interfaces necessary to deliver intercepted communications and call-identifying information [to LEAs]”).

<sup>7</sup> These capabilities, referred to as the DOJ/FBI “punch list,” were: (1) content of subject-initiated conference calls; (2) party hold, join and drop information identifying all active parties to a conference call; (3) subject-initiated dialing and signaling information to inform LEAs of the subject’s use of certain calling features (e.g., call-forwarding and call waiting); (4) in-band and out-

Frontier Foundation, called the standard over-inclusive because it impermissibly included location information and also included packet-mode communications in such a fashion that compliance would enable LEAs to obtain content information “with no more than a pen register order” (*i.e.*, without a Title III warrant, as is required before LEAs may intercept the content of communications).<sup>8</sup>

After the issues were litigated before the Commission and the D.C. Circuit, and then back before the Commission on remand from the D.C. Circuit, the Commission ultimately sided with the DOJ and required that carriers adopt all capabilities of the J-Standard as well as the DOJ/FBI “punch list” capabilities as part of CALEA compliance for wireline, cellular and broadband PCS telecommunications carriers.<sup>9</sup>

With respect to packet-mode communications,<sup>10</sup> the Commission did not require, in either the *Third Report and Order* or in the subsequent *Order on Remand*, any “technical requirements” for those communications (though it did mandate that carriers “implement a packet-mode capability”), but instead “permitted packet-mode data to be delivered to law

---

of-band signaling information containing information about signals sent from the carrier’s network to the subject’s telephone; (5) timing information that would correlate call-identifying information with call content of an intercepted communication; (6) surveillance status information to verify the continuing function of an intercept; (7) continuity check tone to make LEAs aware of the failure of facilities needed to deliver intercepted information; (8) feature status information to advise LEAs of changes in the subject’s subscribed features; and (9) dialed digit extraction information on numbers dialed by the subject after the initial call set-up is completed. *See Third Report and Order* at ¶ 5. *See also United States Telecom Association*, 227 F. 3d at 456.

<sup>8</sup> *United States Telecom Association*, 227 F. 3d at 455-56.

<sup>9</sup> *See In Re: Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, *Order on Remand*, 17 FCC Rcd 6896 at 6897-6899 (2002) (*Order on Remand*).

<sup>10</sup> Under the J-Standard, packet mode communications are described as “a communication where individual packets or virtual circuits of a communication within a physical circuit are switched or routed by the accessing telecommunications system. Each packet may take a different route through the intervening network(s).” *See Third Report and Order* at ¶ 47, n. 97.

enforcement under the [J-Standard].”<sup>11</sup> The J-Standard, in turn, provided for LEA access to call-identifying information and the interception of wire and electronic communications, regardless of the mode employed. The practical effect of the J-Standard, thus, which the Commission (at least temporarily) endorsed, is to establish CALEA packet-mode compliance through the delivery of the full packet stream to law enforcement.

The J-Standard’s “entire packet stream” compliance requirement was hotly contested. Privacy advocates and a number of carriers argued that “any packet-mode data provided to a law enforcement agency pursuant to a pen register order would inevitably include some call content, thus violating CALEA’s privacy protections,” because “packet headers (call-identifying information) cannot be separated from packet bodies or payloads (call content).”<sup>12</sup> Nevertheless, the Commission decided, and the D.C. Circuit affirmed, that although the J-Standard’s approach to packet-mode communications raised significant technical and privacy concerns,” those concerns did not warrant the abandonment of the standard. The Commission did call for “further study” by the standards organizations, however, to address its concerns.<sup>13</sup>

## **2. J-STD-025-B.**

Accepting the Commission’s invitation to study CALEA solutions that would address the Commission’s (and others’) privacy concerns, the standards bodies returned to the drawing board. In December 2003 (once again after extensive discussions and negotiations with the

---

<sup>11</sup> *Id.* at ¶ 55.

<sup>12</sup> *United States Telecom Association*, 227 F. 3d at 464. Interestingly, the DOJ countered this argument by contending that, as a technical matter, it “was perfectly feasible *for a LEA to employ equipment that distinguishes between a packet’s header and its communications payload and makes only the relevant header information available for recording or decoding.*” *Id.* at 465 (emphases added).

<sup>13</sup> *Third Report and Order* at ¶ 55.

DOJ), TIA and ATIS jointly published a new J-Standard -- J-STD-025-B -- to serve as a CALEA safe harbor specifically for packet-mode communications services.

J-STD-025-B focuses on refining the CALEA packet-mode communications requirements for the interface to the collection equipment of LEAs. Several packet-mode technologies fall within the standard's requirements. The standard provides "specific details" of the solution for the CDMA2000 packet data system, and "normative references" to other systems (including wireline VoIP and the wireless systems, Universal Mobile Telecommunications System/General Packet Radio Service (UMTS/GPRS)). J-STD-025-B provides that a packet data intercept access point "shall access data packets transmitted to, or received from the equipment, facilities, or services of an intercept subject when a packet-mode data service is provided."<sup>14</sup>

## **II. LEGAL STANDARDS FOR DOJ'S PETITION.**

As described, Congress deliberately and expressly gave the telecommunications industry the "first crack" at developing the technical standards for CALEA compliance, in lieu of delegating such implementing power to any other entity -- whether law enforcement or the Commission -- in the first instance.<sup>15</sup> This policy choice accommodates Congress' dual objectives of ensuring "efficient and uniform implementation" of CALEA's surveillance assistance requirements "without stifling technological innovation."<sup>16</sup> Thus, even though

---

<sup>14</sup> J-STD-025-B at § 4.6.3. The standard applies to a range of packet data services, specifically including packet-mode services referenced by the Commission in the *Third Report and Order*. Among those listed services are wireless packet-mode data services, including Code Division Multiplex Access or "CDMA" packet-mode service, which is the subject of the DOJ's present Petition. See *Third Report and Order* at ¶ 55, n. 106; J-STD-025-B at § 4.6.3 and § 4.9.1.

<sup>15</sup> *United States Telecom Association*, 227 F. 3d at 460.

<sup>16</sup> *Id.* at 455. See 47 U.S.C. § 1006 (a).

CALEA’s safe harbor provision – Section 107 – assigns a “consultative” role to the DOJ for CALEA standards development, it does not grant the DOJ a standards veto.<sup>17</sup>

Industry-crafted CALEA safe harbors cannot be undone by the Commission without a clear demonstration that they are “deficient”; *i.e.*, that they do not ensure that adopting carriers will meet CALEA’s “*required surveillance capabilities*.”<sup>18</sup> Thus, unless it is shown that a safe harbor standard, if adopted by a carrier, fails to ensure that an adopting carrier’s network will meet the requirements of CALEA (expressly provided in section 103), then the Commission cannot declare the standard to be “deficient.”<sup>19</sup>

Even if a deficiency showing is made, the Commission’s work does not end there, it only begins. The Commission must then craft its own CALEA compliance rules in place of the safe harbor standard, and in doing so, the Commission must ensure that the rules it promulgates: (1) cost-effectively meet CALEA’s assistance capability requirements; (2) safeguard privacy and security of communications not authorized for intercept; (3) minimize costs to ratepayers of compliance; (4) promote U.S. policy of encouraging technological innovation in the provision of services to the public; and (5) establish a reasonable timeframe and conditions for compliance with the new rule, and define carriers’ obligations during the transition from the safe harbor to the Commission’s rules.<sup>20</sup> Both determinations – the finding of a deficiency and that the alternative rule meets the five-part test described above – must be made *before* the Commission may modify a CALEA standard.

---

<sup>17</sup> See *id.* at 455 (“The Act ‘does not authorize any law enforcement agency or officer’ to dictate the specific design of communications equipment, services, or features.”) (citing 47 U.S.C. §1002 (b) (1)).

<sup>18</sup> *Id.* (emphasis added). See 47 U.S.C. § 1006 (b); *Third Report and Order* at ¶ 4.

<sup>19</sup> See *id.* at 454; 47 U.S.C. § 1002 (a).

<sup>20</sup> *Id.* at 455; 47 U.S.C. § 1006 (b). See *Third Report and Order* at ¶ 9.

### **III. DISCUSSION.**

Because AT&T does not utilize CDMA2000 in its wireless network, its stake in the specific technologically-based CALEA issues in this Petition may not be as direct as that of providers that rely upon the technology. Nevertheless, and, particularly in light of DOJ's request that the FCC apply any modifications of the J-STD-025-B standard across the board to all other standards, AT&T files these comments to demonstrate that: (1) the modification of J-STD-025-B proposed by DOJ is inconsistent with the requirements of CALEA; and (2) the FCC cannot lawfully extend any such modification to other standards without undertaking the fact-specific analysis mandated by CALEA with respect to those other standards.

#### **A. "Buffering" (i.e., Storage) Is Not Required By CALEA.**

In its Petition, DOJ asserts that the "loss, omission or corruption of key packets within the subject's communication stream" may compromise law enforcement's surveillance ability, both with respect to call-identifying information and content.<sup>21</sup> From this, the DOJ argues that the J-Standard fails to ensure quantitative performance and reliability measures to address packet loss. DOJ then argues, in a footnote, that these issues could be alleviated by the imposition of a buffering requirement on carriers.<sup>22</sup>

Buffering is merely another name for temporary data storage. In the context of packet-based communications, such storage capabilities are typically used to compensate for the packet

---

<sup>21</sup> Petition at 49.

<sup>22</sup> DOJ also suggests that collocation of law enforcement collection devices in carrier facilities is another potential solution that the Commission could mandate. *Id.* n. 110. DOJ fails to explain, however, how such a mandate would be consistent with section 103(a) (3) of CALEA, which requires carriers to deliver intercepted data to the DOJ "in a format such that they may be transmitted by means of equipment, facilities, or services procured by the DOJ to a location other than the premises of the carrier." (emphasis added).

losses that may result from the “bursty” flow characteristics of packet streams.<sup>23</sup> Under DOJ’s proposal, the use of buffering to mitigate packet loss would presumably entail deploying storage capacity (*e.g.*, a network interface card, a computer or “buffer box”) at particular network nodes to store packets for some unspecified period of time, while they await further transmission to a given LEA’s designated delivery facilities. According to DOJ, such buffering would be “carrier-provided” and the costs of designing, deploying and maintaining the storage media and other aspects of any buffering solution would all be borne by carriers.

As discussed below, DOJ’s buffering proposal is flawed in two significant respects. First, there is no basis in the CALEA statute for imposing a data storage requirement on carriers. Second, even if such a basis could be found, a buffering requirement would impose substantial costs on carriers and, ultimately, their customers.

CALEA requires carriers to be capable of “expeditiously isolating and enabling the DOJ . . . to intercept . . . communications . . . concurrently with their transmission . . . *or* at such later time as may be acceptable to the DOJ,” and of “delivering intercepted communications . . . to the DOJ . . . in a format such that they may be transmitted by means of equipment, facilities, or services procured by the DOJ to a location other than the premises of the carrier.”<sup>24</sup>

The statute’s language thus gives carriers a choice. They may elect to enable a subscriber’s intercepted communications to be delivered to the DOJ concurrently with the interception, or they may elect to enable the intercepted communications to be delivered to the

---

<sup>23</sup> See Newton’s Telecom Dictionary, 21<sup>st</sup> ed., at 135 (“Usually located between two different devices that have different abilities or speeds for handling the data . . . [t]he buffer acts like a dam, capturing the data and then trickling it out at speeds the lower river can handle without, hopefully, flooding or overflowing the banks”).

<sup>24</sup> 47 U.S.C. § 1002 (a) (1) – (3).

DOJ at a “later time as may be acceptable to the DOJ.”<sup>25</sup> DOJ’s buffering proposal would eliminate this choice by forcing carriers to deploy the capability to *both* concurrently transmit intercepted communications to the DOJ and to store intercepted communications for subsequent transmission to the DOJ. The Commission has no authority to rewrite the CALEA statute in the manner DOJ suggests, which would eliminate the flexibility Congress has expressly afforded carriers in meeting their CALEA obligations.

Second, the DOJ’s buffering solution is flawed for practical reasons. As the bandwidth of broadband Internet access services provided to consumers increases over time (*e.g.*, from 1.5 Mbps, to 3 Mbps, to 6 Mbps and beyond), the “carrier-provided” storage capacity contemplated in DOJ’s buffering proposal would need to keep pace with those increases in bandwidth. At the same time, LEAs may request dozens or even hundreds of intercepts operating simultaneously on a single carrier’s network. Thus, a carrier would need to make substantial investments in storage capacity in order to be prepared to satisfy multiple simultaneous intercept requests on its broadband network. DOJ makes no effort to circumscribe the extent of those costs and instead merely asserts – without support – that its proposal is “cost-effective.”<sup>26</sup> Under section 107 (b) (3) of CALEA, however, DOJ has the burden of showing that its proposal would “minimize the cost of . . . compliance on residential rate payers.”<sup>27</sup> DOJ’s failure to even *attempt* to make such a showing is thus a fatal flaw in its Petition.

---

<sup>25</sup> 47 U.S.C. § 1002 (a) (1). Consistent with this statutory choice, CALEA standards bodies have concluded that buffering is “an optional capability” that carriers can implement between the IAP and the DOJ’s collection facilities. *See Technical Report on Data Buffering (Short Term Storage) in an LAES Environment* at 1, American National Standards Institute, Inc., PTSC-LAES-2007-015R5 (October 2006).

<sup>26</sup> Petition at 49, n. 110.

<sup>27</sup> 47 U.S.C. § 1006 (b).

Finally, although DOJ’s “carrier-provided” buffering proposal conflicts with the CALEA statute, there are other buffering options available to DOJ. For example, DOJ could implement a buffering solution using its own facilities. Indeed, section 103 (a) (3) of CALEA expressly contemplates that carriers will deliver intercepted data to “equipment, facilities, or services procured by the DOJ.”<sup>28</sup> Thus, to the extent DOJ or any other LEA desires to implement a buffering solution, they are free to do so.

**B. “Packet Activity Reporting” Is Burden-Shifting By Another Name.**

DOJ charges that J-STD-025-B fails to provide for “packet activity reporting.”<sup>29</sup> According to DOJ, “packet activity reporting” capabilities would consist of “IP addresses, port numbers, and transport layer protocol information for the source and destination of an IP packet.” Without citing CALEA, the J-Standard or other authoritative source, DOJ declares that “packet activity reporting” is compelled by CALEA because it “refers to a carrier’s ability to isolate and deliver the [call-identifying information] contained in IP communications packets that are sent by or to an intercept subject.”<sup>30</sup>

Wherever the “packet activity reporting” concept comes from, it is clear from the CDMA2000-specific J-Standard requirements that the information demanded by the DOJ *is* provided to it, albeit perhaps in “payload” packets within the “entire packet stream” in some respects, per the DOJ’s lawfully authorized requests. J-STD-025-B requires that carriers make available both header and payload – *i.e.*, the entire packet stream – to LEAs for all packet-mode technologies, including CDMA2000 and other wireless packet-mode technologies. Thus, far

---

<sup>28</sup> 47 U.S.C. § 1002 (a) (3).

<sup>29</sup> *See* Petition at 12-18.

<sup>30</sup> *Id.* at 12.

from making a case that it is not receiving data packets to which it is entitled, the DOJ is arguing that, unless the data is decoded, separated and presented to it in the fashion it demands (*i.e.*, in a way that does not require it to extract anything), a carrier is not complying with CALEA.

The DOJ's argument rests on an insupportable interpretation of the CALEA statute. Section 103 says that carriers must "expeditiously isolate[e] and enable[e] the DOJ . . . to access call-identifying information that is reasonably available to the carrier." If the DOJ is getting the packet stream that *contains* readily available call-identifying information (in addition to typical header information that is also provided), the DOJ cannot claim that that information in hand has not been effectively "isolated." "Isolated" does not mean "decoded," "separated," or the like, as the DOJ implicitly suggests. Indeed, when one looks at the immediately preceding capability requirement in Section 103 relating to content, it is clear that "isolation" when used in that section means apart from, or exclusive of, communications information *that the DOJ is not authorized to have*.<sup>31</sup>

Moreover, and to the extent that the term "isolating" as used in section 103 (a) (2) might arguably have a materially different meaning than that assigned to it in section 103 (a) (1), further language in (a) (2) indicates that, at most, "isolating" means that the information will be made available to the DOJ "in a manner that allows it to be associated with the communication to which it pertains."<sup>32</sup> If the information is included within the packet stream, as it undeniably is, then the DOJ cannot possibly suggest that it is deprived of the ability to "associate the information with the communication to which it pertains."

---

<sup>31</sup> See 47 U.S.C. § 1002 (a) (1) (carriers must ensure that it is capable of "expeditiously isolating and enabling the DOJ . . . to intercept to the exclusion of any other communications . . .").

<sup>32</sup> 47 U.S.C. § 1002 (a) (2) (B).

The extraction, classification and ordering of packet-mode data for the DOJ is *not* required by CALEA. The statute nowhere states that, with respect to packet-mode communications, carriers must decode the packets at their own expense. To the contrary, to the extent DOJ undertakes these activities, it must do so at its own expense.<sup>33</sup>

**C. Disposition of the Present J-STD-025-B Question In Favor of DOJ Should Not Be Automatically Applicable to Other CALEA Standards.**

The DOJ, in footnote 10 at page 5 of its Petition, contends that “any rules established by the Commission requiring carriers to provide the additional and/or modified capabilities described herein should also be applicable with respect to other published standards where the same capabilities are at issue.”<sup>34</sup> Any such requirement would be inconsistent with CALEA’s terms, and arbitrary and capricious.

If the DOJ prevails in establishing that J-STD-025-B is deficient, which it should not, it will be based on specific showings germane to *that* standard and the surveillance requirements and network issues *that* standard addresses. It would not automatically translate to other CALEA industry standards. To the contrary, those other standards would have to be evaluated on their own merits and the full analysis required by the CALEA statute would need to be conducted before any finding of deficiency could be made.

---

<sup>33</sup> What the DOJ does correctly suggest, however, is that the imposition of a decoding requirement upon carriers will result in an extraordinary expense that, ultimately, will be borne by their customers through higher bills. Large data delivery pipes would be needed for the additional data collection and transport burdens that would result from the DOJ’s requirements being made into law. And, carriers would all presumably need to re-design and re-engineer their packet data networks to perform the summaries that the DOJ inherently seeks in its “packet activity reporting” mandate. The issue is who has to invest in these capabilities – the DOJ or the carriers. Carriers are already meeting CALEA’s requirements by ensuring that the data is passed along to LEAs pursuant to lawful requests; nothing more is required of them.

<sup>34</sup> Petition at 5, n. 10.

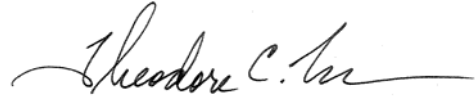
For example, law enforcement and industry have been engaged in extensive and detailed discussions for several years on the issue of buffering/storage. Those discussions have been a part of the development of a proposed LAES standard that have seen law enforcement move from an initial request of a five-day storage requirement to a 24-hour requirement. At present, the standards body has issued a technical report on buffering (referenced herein) which is the focus of active discussion between enforcement and industry. That report, at present, makes buffering an optional capability that carriers can provide to LEAs, but the entire matter is undergoing extensive debate at the present time and is subject to further change and developments.

For the reasons discussed herein, and for broader reasons of network design, architecture, cost, *etc.*, there is no basis to conclude that a buffering solution that might work for CDMA2000 would work for any other wireless technology or, for that matter, wireline packet technology. Those matters would have to be studied intensively before a determination could be made on a proper solution and, as discussed, industry must be given “first crack” at the development of standards for those solutions. The DOJ’s automatic applicability approach, thus, not only would circumvent CALEA’s requirements, but would certainly lead to the enunciation of a rule whose technical viability could not be demonstrated. To avoid such an unlawful and counterproductive outcome, the Commission should reject DOJ’s request for the automatic applicability approach.

**IV. CONCLUSION**

For the foregoing reasons, the Commission should deny DOJ's Petition.

Respectfully submitted,

A handwritten signature in cursive script, reading "Theodore C. Marcus", is written over a horizontal line.

Theodore C. Marcus  
Jack Zinman  
Gary L. Phillips  
Paul K. Mancini

AT&T Inc.  
1120 20th Street, N.W.  
Suite 1000  
Washington, DC 20036  
(202) 457-2044  
Its Attorneys

July 25, 2007