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

| | |
|---|---|
| In the Matter of<br><br>Petition for Expedited Rulemaking to Establish Technical Requirements and Standards Pursuant to Section 107(b) of the Communications Assistance for Law Enforcement Act | RM-11376 |

**JOINT COMMENTS SUBMITTED ON BEHALF OF**

**AMERICAN LIBRARY ASSOCIATION, ASSOCIATION OF RESEARCH LIBRARIES, CENTER FOR DEMOCRACY & TECHNOLOGY, CHAMPAIGN-URBANA COMMUNITY WIRELESS NETWORK, ELECTRONIC FRONTIER FOUNDATION, MEDIA ACCESS PROJECT, THE RUTHERFORD INSTITUTE, and THE VOICE ON THE NET (VON) COALITION**

James X. Dempsey
John B. Morris, Jr.
Center for Democracy & Technology
1634 I Street, NW, Suite 1100
Washington, D.C. 20006
(202) 637-9800

Dated: July 25, 2007

## TABLE OF CONTENTS

## SUMMARY

In its "Petition for Expedited Rulemaking," the U.S. Department of Justice asks this Commission to go far beyond what is allowed by the Communications Assistance for Law Enforcement Act ("CALEA"), and to impose on Internet access providers (including the CDMA2000 providers discussed in DOJ's Petition) CALEA obligations that far exceed what law enforcement is able to obtain using CALEA in the PSTN context.

As a threshold matter, the Commission must reject DOJ's effort to do an end run around both CALEA and the Administrative Procedures Act by extending any rules far beyond the CDMA2000 context that is ostensibly the focus of DOJ's Petition. The Commission must limit this proceeding to the specific standard challenged by DOJ, ANSI's J-STD-035-B.

On the substance of DOJ's challenge to the J-STD-025-B standard itself, the Commission should reject all of DOJ's requests:

**"Packet Activity Reporting":** Contrary to DOJ's argument, "packet activity reporting" cannot be deemed to be "Call-Identifying Information" ("CII") in the context of CALEA obligations of a provider of *access* to the Internet. The crucial element of Commission's extension of CALEA to Internet access providers (and the decision by the Court of Appeals to uphold the Commission) is that the "transmission" portion of Internet access service is separate from the information services portion, and CALEA can be applied to the transmission portion. In its Petition, DOJ asks this Commission to do a 100% about face, and to merge information services back into the transmission services for CALEA purposes. But as the Court of Appeals made crystal clear, the transmission services are the *only* part of Internet access that can be reached by CALEA. Extending CALEA to the information services portion would give DOJ far

more than it receives in the comparable situation in the PSTN context, and would violate CALEA.

**Port Numbers:** "Call-Identifying Information" cannot under CALEA include the content of a communications. For a CDMA2000 access service provider, port numbers are *content*, and thus cannot be covered by CALEA. Again, DOJ is asking the Commission to give it far more in the Internet access context than it receives in the PSTN context.

**200 Millisecond "Accuracy" in Time Stamps:** Although the start and stop time of a communication is appropriately included in CII, it is both burdensome and wholly unnecessary to require access providers to provide time stamps with an "accuracy" or "precision" of 200 milliseconds. DOJ ignores the fundamental reality about the Internet – that unlike the PSTN the Internet does not require highly accurate and closely synchronized timing for communications to flow. Granting DOJ's Petition on this point would require a sweeping revamping of Internet access providers' networks, and the Internet as a whole. The Commission lacks the authority for such a sweeping mandate.

**Heightened Location Precision:** DOJ's request for the Commission to impose a heightened degree of location accuracy was squarely rejected in 1999 and 2000 by both the Commission and the U.S. Court of Appeals, and DOJ points to *nothing* to suggest that the legal or privacy considerations have in any way changed on this point since 1999. DOJ now asks the Commission to go much farther than what the Commission rejected in 1999. DOJ's Petition, if granted, would directly harm the day-to-day privacy of millions of wireless uses across the country. The Commission should reaffirm its 1999 decision and reject DOJ's Petition.

**Cost Shifting:** The Commission must reject DOJ's efforts to impose on carriers costs that the CALEA statute itself makes clear are costs that must be born by the government.

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

| | |
|---|---|
| In the Matter of<br><br>In the Matter of Petition for Expedited Rulemaking to Establish Technical Requirements and Standards Pursuant to Section 107(b) of the Communications Assistance for Law Enforcement Act | RM-11376 |

**JOINT COMMENTS SUBMITTED ON BEHALF OF**

**AMERICAN LIBRARY ASSOCIATION, ASSOCIATION OF RESEARCH LIBRARIES, CENTER FOR DEMOCRACY & TECHNOLOGY, CHAMPAIGN-URBANA COMMUNITY WIRELESS NETWORK, ELECTRONIC FRONTIER FOUNDATION, MEDIA ACCESS PROJECT, THE RUTHERFORD INSTITUTE, and THE VOICE ON THE NET (VON) COALITION**

American Library Association, Association of Research Libraries, Center for Democracy & Technology, Champaign-Urbana Community Wireless Network, Electronic Frontier Foundation, Media Access Project, The Rutherford Institute, and The Voice On The Net (VON) Coalition respectfully submit these comments in opposition to the "Petition for Expedited Rulemaking" filed by the U.S. Department of Justice ("DOJ") on May 15, 2007, pertaining (ostensibly) to the J-STD-025-B standard for compliance with the Communications Assistance for Law Enforcement Act ("CALEA").[1]

[1] Pub. L. No. 103-414, 108 Stat. 4279 (1994), *codified as* 47 U.S.C. §§ 1001-10 and 47 U.S.C. § 229.

## I. THE COMMISSION MUST REJECT THE EFFORT BY THE DEPARTMENT OF JUSTICE TO DO AN END RUN AROUND BOTH CALEA AND THE ADMINISTRATIVE PROCEDURES ACT.

In the first paragraph of its Petition and then repeatedly throughout its 66 page filing, the Department of Justice aims its arguments at ANSI's "J-STD-025-B, the CALEA standard for CDMA2000 packet data wireless service." Petition at 2 *et seq.* Yet in footnote 10 of its Petition, DOJ asserts that "any rules established by the Commission [in response to the Petition] should also be applicable" to other standards where the same capabilities are at issue. Thus, although claiming to focus on CDMA2000 service, DOJ is in fact seeking an advance ruling invalidating a host of unidentified standards, some of which may not have even been created yet. Under both CALEA and the Administrative Procedures Act, the Commission must reject this gambit.

Under CALEA, the Commission's sole statutory authority is this regard is to respond to a deficiency petition pertaining to a specific failure to create a standard, or a specific asserted deficiency in a standard. *See* CALEA § 107(b). DOJ has only come forward with assertions about a single standard, and the Commission's authority is limited to that standard. Moreover, under the Administrative Procedures Act, a single footnote in a 66-page long petition is inadequate to give appropriate notice to the public, or to individuals and entities that might be affected by an as-yet-unidentified range of other standards that DOJ seeks to cover.

Looking at just one of DOJ's claims against the J-STD-025-B standard highlights the wisdom behind CALEA's requirement that the Commission only consider a single standard at a time. DOJ seeks to impose on CDMA2000 systems a requirement that a provider report a time stamp to an "accuracy" of 200 milliseconds. *See* Petition at 19-20. Whether that is an appropriate requirement in the wireless CDMA2000 context (and as discussed below, it is not), such a requirement would be extraordinarily burdensome in other contexts involving "wired" ISPs – many of which operate networks that in their current form only have the capability to time

events to a precision of 1 second. In those contexts, a rule requiring such timing could require ISPs to replace many if not all of the switches and routers in their networks, at extraordinary expense (for, as discussed below, a functionality that is largely unnecessary in the Internet context).

As the CALEA statute recognized, different standards may be necessary in different technological contexts. The Commission should not, and cannot, allow DOJ to try to expand this processing beyond the CDMA2000 standard.

## II. THE "PACKET ACTIVITY REPORTING" SOUGHT BY DOJ IS *NOT* "CALL-IDENTIFYING INFORMATION" THAT THE COMMISSION CAN REQUIRE TO BE PRODUCED UNDER CALEA; TO ORDER ITS INCLUSION AS CII WOULD VIOLATE BOTH CALEA AND THE U.S. COURT OF APPEALS DECISION APPLYING CALEA TO BROADBAND ACCESS PROVIDERS.

In asking this Commission in 2004 (and ultimately the Court of Appeals) to extend CALEA to broadband access service, DOJ repeatedly argued that it was simply trying to replace what it lost in the PSTN – the ability to capture a target's telephone call to his ISP.[2] DOJ argued that broadband was a "substantial replacement" for dial-up access to the Internet, and that is what this Commission held. The Commission itself then spent *eleven pages* of its main brief to the U.S. Court of Appeals in 2006 to argue that its application of CALEA to broadband access was permissible based on the Commission's separation of the underlying transmission function of broadband access from the excluded information services.[3] The Court of Appeals in turn relied on both DOJ's and the Commission's arguments and made specifically clear in its holding that it

[2] *See, e.g.,* Reply Comments of the United States Department of Justice, at 15, *In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services,* filed Dec. 21, 2004 (ET Docket No. 04-295) [hereafter "DOJ Reply Comments"]; Brief for Respondent United States, at 23, *American Council of Education v. Fed. Communications Comm.*, filed Feb. 27, 2006 (D.C. Cir. No. 05-1404).

[3] *See* Brief for Respondent Federal Communications Commission, at 26-37, *American Council of Education v. Federal Communications Commission*, filed Feb. 27, 2006 (D.C. Cir. No. 05-1404).

was *only* the transmission function of broadband access that was covered by CALEA. The court specified exactly what part of broadband access was covered by CALEA:

> [t]he "switching and transmission" portion of a broadband service offering—which replaces the "switching or transmission" portion of a dial-up Internet connection . . . .[4]

Without this critical distinction between transmission and the underlying information services – argued by DOJ, accepted by this Commission, and then upheld by the Court of Appeals – CALEA by its terms could not apply to Internet access.

In its Petition asking for what it calls "packet activity reporting," DOJ asks this Commission to adopt a 100% change in course, and to completely abandon the core distinction between the transmission service and the underlying information service. DOJ is asking the Commission to order that the *transmission service provider* (the broadband access provider) be required under CALEA to produce "call-identifying information" for the underlying information services. This is *exactly* contrary to the very basis of the Commission's extension of CALEA to broadband access, and the Court of Appeals decision upholding that extension. The Commission should reject DOJ's Petition out of hand.

To appreciate the magnitude of DOJ's about face, consider DOJ's original argument in 2004 to extend CALEA to broadband access: broadband access to the Internet was a "substantial replacement" for dial-up access, and thus the FCC needed to ensure that people who used to use dial-up access to reach the Internet could not avoid CALEA by using broadband access. As noted, DOJ repeatedly claimed that it simply was trying to replace what it "lost" when Internet access started moving from dial-up to broadband. But DOJ is now seeking much, much more.

---

[4] *American Council of Education v. Federal Communications Commission*, 451 F.3d 226, 234 (D.C. Cir. 2006).

It is critical to note exactly what DOJ had under CALEA before broadband: CALEA required a local exchange carrier ("LEC") to meet CII obligations with regard to a target's telephone call to reach his or her dial-up ISP. The LEC had to provide certain information about the start of that telephone call, and the end of that telephone call, but the LEC had *no obligation whatsoever* to listen in on the telephone call and provide "packet activity reporting" on every Internet packet that traveled over the LEC's *transmission* facilities. All the LEC – the transmission service provider – had to do was to report information about the *transmission* itself, not about what packets were carried in the transmission. But that is now *exactly* what DOJ is asking the Commission to require wireless *transmission service providers* to do. Contrary to all of its prior arguments to the Commission and the Court of Appeals, DOJ is now asking the Commission to merge information service back into transmission services, and make the transmission service provider subject to CALEA obligations with regard to the information services portion of broadband access. Were this Commission to grant DOJ's Petition, the Commission would be acting directly contrary to the holding of the U.S. Court of Appeals.

Moreover, were the Commission to grant DOJ's Petition, DOJ would presumably turn around and file a deficiency petition challenging the *J-STD-025-A* standard that covers telephone calls to dial-up ISPs. In terms of Internet access, there is no functional difference between the CDMA2000 wireless provider covered by J-STD-025-B and the LEC covered by J-STD-025-A, and there is no legal foundation in CALEA for treating them any differently. Either both J-STD-025-A and J-STD-025-B are deficient in this regard, or neither is deficient. Either both LECs and CDMA2000 service providers must break into the *transmission* of IP packets and provide "packet activity reporting," or neither type of provider must do so. It is presumably beyond question, however, that the LEC cannot be made under CALEA to break the dial-up Internet call

into individual packets, and it should be equally beyond question that CDMA2000 providers cannot be required under CALEA to do the same thing.

The CDMA2000 standard challenged in this Petition provides DOJ with *exactly* the same type and quantity of information that DOJ receives under CALEA/CII in the dial-up Internet scenario. And this is *exactly* what DOJ asserted to both this Commission and the Court of Appeals that is was seeking by asking the Commission to extend CALEA to broadband access. DOJ cannot ask for a complete change of course now.

To be clear, DOJ is absolutely able to serve lawfully authorized pen/trap warrants to obtain "call-identifying information" pertaining to information services. In other words, if DOJ obtains from a court a proper pen/trap order applicable to a target's entire Internet data stream (which would have to exclude the content elements that are revealed in that data stream), then DOJ can obtain reports on "packet activity" that it addresses here. But, critically, it must obtain such information from the information service provider *not* the transmission provider, and it cannot impose CALEA obligations to require the information service provider to redesign its network to meet DOJ demands.

The fact that in many broadband contexts (including CDMA2000) the transmission service provider is often vertically integrated with the information service provider does not change the CALEA analysis. Indeed, both the Commission and Court of Appeals decisions were specifically hinged on the holdings that such integrated providers had two separate functions, and that CALEA treated those functions differently. DOJ cannot have its cake and eat it too – it cannot ask for separate functional treatment to claim that CALEA applies to broadband access,[5]

[5] *See, e.g.,* DOJ Reply Comments, at 15-16 (arguing that vertical integration of transmission providers and information service providers did not justify excluding the transmission services from CALEA).

and then ask for unitary functional treatment when analyzing *how* CALEA applies to broadband access. DOJ's Petition seeking "packet activity reporting" must be denied.

## III. DOJ'S "PACKET ACTIVITY REPORTING" "PUNCH LIST" INCLUDES ITEMS THAT SHOULD NOT BE DEEMED TO BE CII IN THE INTERNET ACCESS CONTEXT.

If the Commission rejects DOJ's request to impose "packet activity reporting" on CDMA2000 transmission providers – as it should – the Commission need not address some of the more specific requests about details of such reporting. But if the Commission determines that it should address those issues, the undersigned urge the Commission to reject, at a minimum, (a) DOJ's suggestion that "port numbers" are CII in the access context, and (b) DOJ's demand that time stamps be provided with 200 millisecond "accuracy."

### A. Port Numbers are Not Appropriately Viewed at CII for a CDMA2000 Transmission Service Provider.

DOJ asserts in its Petition that "port numbers" – information that in many cases indicates what "type" of Internet communication is being sent – should be deemed to be CII for purposes of the CALEA obligations of CDMA2000 transmission service providers. *See* Petition, as 12-16. Port numbers, however, are not used by those providers of transmission services in the transmission of the communications, and in any event they provide information about the *content* of the communication – information that cannot be included in CII under CALEA.

Again, it is critical to note exactly what DOJ had under CALEA before broadband: A local exchange carrier had no obligation to break into a phone call and determine what *type* of phone call it was – whether it was a voice call, a fax call, a modem call, for example. Moreover, the LEC certainly has no obligation to listen to a call to a dial-up ISP and report the port number

of the IP packets (just as it does not have the broader obligation to report on each packet, as discussed above).

In the PSTN, the *type* of phone call is irrelevant to the transmission services provided by the LEC, and is a critical element of the *content* of the call itself. In the PSTN context, CALEA does not require LECs to listen in on a phone call and report as CALEA required-CII the *type* of the call. But this is exactly what DOJ asks the Commission to impose *as CII* on CDMA2000 providers. The Commission does not have the authority under CALEA to redefine elements of the content of a communication and make them part of "call identifying information."

Again, to be clear, port numbers may well be appropriately obtainable under a pen/trap order *served on an information service provider*. And thus DOJ can certainly – if it obtains the appropriate court order applicable to the appropriate entity – obtain the port numbers it asserts that it needs. What it cannot do is obtain port numbers as CII *from the transmission provider under CALEA*. DOJ's effort to obtain port numbers from CDMA2000 providers must be rejected.

### B. DOJ's Demand for 200 Millisecond Time Stamp Accuracy Is Both Unnecessary And Wholly Inconsistent With How The Internet Operates.

Another key element of the "packet activity reporting" that DOJ seeks is "time stamp" information with an "accuracy"[6] of 200 milliseconds. Commenters readily agree that DOJ can obtain as CII the start and end time of a call, but in the Internet context it is wholly unreasonable

[6] It is very unclear from DOJ's Petition whether they are complaining about the "accuracy" or "precision" of the time stamp, or possibly both. Confusion between these two terms is common, as suggested by the numerous Internet web sites devoted to explaining the difference between the terms. *See, e.g.,* http://www.ece.unb.ca/tervo/ee2791/intro.htm ("The precision of an instrument reflects the number of significant digits in a reading; [t]he accuracy of an instrument reflects how close the reading is to the 'true' value measured."). It appears more likely that DOJ means "precision," but the comments that follow demonstrate that *both* precision and accuracy of 200 milliseconds are unnecessary and inappropriate in the Internet context.

to seek to impose a time stamp requirement more "accurate" (or more correctly, "precise") than 1 second. And indeed, the very notion of "accurate" time stamps in the Internet context ignores the fact that time synchronization is *not* a required or widespread part of the Internet. At its core, DOJ's argument for 200 millisecond time stamps is that "we have it on the PSTN and so we must have it on the Internet," without (as is statutorily required) taking into account the radical differences between the PSTN and IP networks.

Unlike in the circuit switched world, the Internet infrastructure does not need its network elements to be time-synchronized. A router or a switch that thinks the time at a given point is, say, 09:37:*43* (reported with a one second level of precision), can exchange packets with another router or switch that thinks the time is 09:37:*58* at the same point in time. In other words, the fact that separate network components do not agree on what time it is *does not matter* in the Internet – packets will flow back and forth without difficulty. This is true both between different network operators *and* within a single network. Indeed, a fundamental feature of the TCP/IP suite of protocols is that it permits asynchronous communications, and that it does not require any time synchronization between elements in order to exchange packets.

Thus, because timing is not a significant concern in basic Internet communications, it is common for routers, switches, and other elements used across the Internet not to report or track the time to a higher degree of precision than one second. Although *some* ISPs may seek to maintain a higher degree of time accuracy (to, for example, be able to compare security logs across a network), such practices are not required and cannot be mandated without imposing significant burdens. To require a precision down 200 milliseconds as a routine matter could force some service providers to replace significant amounts of hardware to comply with such a requirement.

Moreover, precise (or accurate) time stamps are unnecessary on the Internet, when IP packets have correlation IDs that allow separate packets to be associated even when they arrive at separate times. In the circuit switched world, law enforcement at times *does* need highly precise timing in order to correlate a content interception with the associated signaling information. But in the Internet context, such correlation is an inherent part of essentially all Internet protocols that use more than one packet. Thus, if DOJ obtains a warrant to obtain the content of a communication on the Internet, the needed correlation information will be delivered to law enforcement *wholly apart from any timing information*.

DOJ's Petition speaks of "accuracy" when seeking a time stamp with – using the more appropriate term – a "precision" of 200 milliseconds. "Precision" in the time context means how granular a time is reported – whether time is, for example, recorded by the minute, by the second, or by the millisecond. "Accuracy" is an entirely different question – whether a reported time is in fact "correct" according to some external "true" time (such as an agreed upon atomic clock). As noted above, however, there is no need for "accurate" time in order to send communications over the Internet. Although some Internet *applications* can benefit from accurate time – and the Network Time Protocol ("NTP") can facilitate the needed level of accuracy – such accuracy is *not* needed for the underlying Internet communications. If DOJ is suggesting that CII time stamps must be "accurate" across the Internet – including either within a single network or across unrelated networks – then DOJ is proposing a complete reworking of how the Internet operates. The Commission does not have any authority – under CALEA or any other statute – to order such a revamping of the Internet.

## IV. THE HEIGHTENED LOCATION REQUIREMENT SOUGHT BY DOJ IS NOT REQUIRED BY CALEA, AND WOULD REQUIRE A RADICAL RESTRUCTURING OF CURRENT LOCATION PRACTICES – RESULTING IN A GROSS AND ON-GOING VIOLATION OF USERS' PRIVACY.

In its Petition, DOJ asks the Commission to revisit the 1999 rejection by the Commission of law enforcement's efforts to receive location information that is more precise or granular than cell tower location. In its 1999 Third Report & Order, the Commission weighed privacy concerns raised by law enforcement's call for more granular information, and specifically rejected the call because it would "undermine individual privacy."[7] Privacy advocates challenged even the degree of location information that the Commission did require in 1999, and in 2000 the U.S. Court of Appeals affirmed the Commission's privacy determination, citing to the privacy mandate in CALEA itself.[8]

Nothing has happened since 1999 or 2000 to change this privacy determination, and DOJ does not even attempt to identify any change to the statutory privacy mandate in CALEA. DOJ fails to advance *any* legal analysis that would warrant revisiting – much less overturning – the 7+ year-old determinations by this Commission and the U.S. Court of Appeals that the Commission had struck the statutorily proper privacy balance in 1999. Until and unless DOJ presents affirmative argument that some legal or statutory change requires a redetermination of this settled issue, the Commission should not consider DOJ's request.

Instead of addressing the statutorily mandated privacy determination made by the Commission in 1999, DOJ's only argument is that – supposedly – technology has progressed since 1999. But this completely ignores the facts that (a) more precise location technology *was*

[7] Communications Assistance for Law Enforcement Act, *Third Report and Order* ¶ 46, CC Docket No. 97-213, 14 FCC Rcd 16794 (1999).

[8] *U.S. Telecom Ass'n v. Federal Communications Commission*, 227 F.3d 450, 463-64 (D.C.Cir. 2000).

available in 1999,[9] and (b) law enforcement's call to require use of that more precise technology was rejected *on legal, privacy grounds*, not because of the state of location technology. DOJ's assertion that technology has changed is some significant manner since 1999 is neither true nor relevant.

Notwithstanding its complete failure to address the privacy determination of the Commission and the Court of Appeals, DOJ in its Petition makes a far more aggressive and far more privacy-invasive proposal than was rejected 7+ years ago. The sweeping destruction of Americans' privacy that DOJ proposes is breathtaking. On page 33-34 of it Petition, DOJ essentially asks the FCC to override the privacy choices made by millions of Americans who use GPS-enabled wireless handsets.

In its Petition, DOJ argues that the Commission should require carriers to provide under CALEA the "highly accurate geographical (latitude-longitude)" location information that can be delivered – often by use of a GPS chip – in the event of a e911 call. *See* Petition at 33-34 & n.83. But to provide such information, wireless carriers would have to force users to always have the GPS capability turned on.

In almost all GPS-enabled wireless handsets sold in this country today, users are give the following specific choice (or similar words) about when to have the phone's internal GPS capability activated:

*** Location Always On** [or]
*** 911 only**

Under DOJ's Petition, CDMA2000 carriers would be required to remove that choice, and force all wireless users to have "Location Always On" (instead of having the GPS chip activated *only*

[9] The Court of Appeals specifically referenced the more precise location technology advocated by New York law enforcement authorities in 1999. *See USTA v. FCC*, 227 F.3d at 463-64.

for e911 calls).[10] Such a requirement would radically increase the risk of both commercial and governmental abuse of this on-going tracking capability – notwithstanding DOJ's assertion that it is not at this time seeking that capability. It would also squarely violate the explicit probation in CALEA on allowing law enforcement to "to require any specific design of equipment, facilities, services, features or system configurations." CALEA § 103(b)(1); 47 U.S.C § 1002(b)(1).

Beyond the harm to privacy, a CALEA location mandate would harm innovation in at least two ways. First, any requirement that carriers implement any specific location technology would hamper the potential for new and innovative location technologies. Second, any requirement that *carriers* must have access to GPS location information used by location based services would chill the creation of third party location service providers (which could provide innovative services, and could provide enhanced privacy guarantees to users). Congress was clear in its intent to avoid technology mandates and protect technological innovation under CALEA. In fact, Congress specifically stated that its "intent is that compliance with the requirements in [CALEA] will not impede the development and deployment of new technologies."[11] Under CALEA, Congress made explicit that law enforcement may neither dictate system design features and nor bar introduction of new features and technologies.[12] The Commission must respect Congressional intent to not impede innovation, and therefore not impose any specific technology or technological solution for CALEA implementation.

[10] It would not be possible for the carrier to "turn on" the GPS chip only for the purpose of executing a wiretap – because such action would be readily detectable by the targeted wireless subscriber (thereby violating the secrecy requirement in CALEA). And if Commission were to make CALEA location disclosure a condition of any location based service, it would likely significantly chill the market for such services.

[11] House Report 103-827, "Telecommunications Carrier Assistance to the Government," Oct. 4, 1994, at 19; Senate Report 103-402, "The Digital Telephony Bill of 1994," Oct. 6, 1994, at 19.

[12] *Id.*

The Commission correctly rejected law enforcement's effort to impose stringent location requirements in 1999, and the Court of Appeals affirmed that determination. The Commission should reject out of hand the even more Orwellian proposal advanced by DOJ in its current Petition.

## V. DOJ'S DEMAND THAT THE COMMISSION REQUIRE CO-LOCATION OR CARRIER STORAGE OF INTERCEPTED COMMUNICATIONS IS NOT PERMITTED BY CALEA, AND IS SIMPLY DOJ'S EFFORT TO SHIFT THE COST AND BURDEN OF INTERCEPTING LARGE VOLUMES OF DATA.

In their discussion of "security, performance and reliability capabilities," DOJ requests that the Commission impose on CDMA2000 carriers an enormous additional burden, in the form of either mandated co-location of interception equipment or required storage by the carriers of intercepted data. Neither proposed requirement is permitted by CALEA, and both simply reflect DOJ's effort to avoid the clear and unavoidable requirement that means of transmittal of intercepted data must be "*procured by the government*" and not the carrier. 47 U.S.C. § 1002(a)(3). Simply stated, if DOJ wants to intercept a large volume of data, it – and not the carrier – is responsible for arranging and paying for the facilities to carry that data "to a location *other than the premises of the carrier." Id.* The Commission has no authority to impose this burden on carriers.

This demand by DOJ is even more problematic if any of these proposed rules were to be applied outside of the CDMA2000 context. In the wake of the recent closure of the second largest VoIP provider in the country,[13] the Commission should not be considering placing greater financial and regulatory burdens on Internet access or other IP services.

[13] *See* "SunRocket Goes Out of Business, Leaving Customers in the Lurch," Washington Post, p. D4 (July 18, 2007).

## CONCLUSION

For the foregoing reasons, the Commission should reject the DOJ's Deficiency Petition challenging the J-STD-025-B standard as a CALEA safe harbor.

ON BEHALF OF

AMERICAN LIBRARY ASSOCIATION (www.ala.org)
ASSOCIATION OF RESEARCH LIBRARIES (www.arl.org)
CENTER FOR DEMOCRACY & TECHNOLOGY (www.cdt.org)
CHAMPAIGN-URBANA COMMUNITY WIRELESS NETWORK (www.cuwin.net)
ELECTRONIC FRONTIER FOUNDATION (www.eff.org)
MEDIA ACCESS PROJECT (www.mediaaccess.org)
THE RUTHERFORD INSTITUTE (www.rutherford.org)
THE VOICE ON THE NET (VON) COALITION (www.von.org)

Respectfully submitted by,

/s/

James X. Dempsey
John B. Morris, Jr.
Center for Democracy & Technology
1634 I Street, NW, Suite 1100
Washington, D.C. 20006
(202) 637-9800

Dated: July 25, 2007