

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

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

**REQUEST FOR STAY PENDING ISSUANCE OF SUBSEQUENT ORDERS  
AND FOR STAY PENDING JUDICIAL REVIEW**

**SUBMITTED ON BEHALF OF**

**CENTER FOR DEMOCRACY & TECHNOLOGY, AMERICAN LIBRARY  
ASSOCIATION, ASSOCIATION FOR COMMUNITY NETWORKING, ASSOCIATION  
OF COLLEGE AND RESEARCH LIBRARIES, ASSOCIATION OF RESEARCH  
LIBRARIES, CHAMPAIGN URBANA COMMUNITY WIRELESS NETWORK,  
ELECTRONIC FRONTIER FOUNDATION, ELECTRONIC PRIVACY  
INFORMATION CENTER, PULVER.COM, SUN MICROSYSTEMS and TEXAS  
INTERNET SERVICE PROVIDERS ASSOCIATION**

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

(counsel continued on following page)

Dated: November 23, 2005

Albert Gidari  
Perkins Coie LLP  
1201 Third Avenue, Suite 4800  
Seattle, Washington 98101  
(206) 359-8688  
Counsel for American Library Association,  
Association of College and Research  
Libraries, and Association of Research  
Libraries

Andrew J. Schwartzman  
Harold Feld  
Media Access Project  
1625 K Street NW, Suite 1000  
Washington, DC 20006  
(202) 232-4300  
Counsel for Association For Community  
Networking, Champaign Urbana  
Community Wireless Network, and  
Texas Internet Service Providers  
Association

Lee Tien  
Kurt B. Opsahl  
Electronic Frontier Foundation  
454 Shotwell Street  
San Francisco, CA 94110  
(415) 436-9333  
Counsel for Electronic Frontier Foundation

Marc Rotenberg  
Sherwin Siy (admission pending in Calif.)  
Electronic Privacy Information Center  
1718 Connecticut Ave. NW, Suite 200  
Washington, DC 20009  
(202) 483-1140  
Counsel for Electronic Privacy  
Information Center

Jonathan Askin  
pulver.com  
115 Broadhollow Road, Suite 225  
Melville, NY 11747  
(631) 961-1049  
Counsel for pulver.com

**TABLE OF CONTENTS**

**SUMMARY**..... **iii**

**BACKGROUND**..... **2**

**REASONS FOR A STAY**..... **4**

**I. IT WAS ARBITRARY AND CAPRICIOUS TO FORCE ENTITIES TO BEGIN COMPLYING WHILE DEFERRING TO AN UNCERTAIN FUTURE DATE DECISIONS AS TO WHAT “COMPLIANCE” MEANS, WHO EXACTLY IS COVERED, AND WHO IS ENTITLED TO AN EXEMPTION**..... **5**

A. The 18 Month Deadline, as the Average of Uninformed Estimates, is Itself Arbitrary and Capricious ..... 6

B. It is Arbitrary and Capricious to Require Entities to Begin Compliance Measures Without Telling Them What Compliance Means ..... 7

C. By Immediately Setting a Compliance Deadline, the Commission Arbitrarily and Capriciously Delegated to the FBI the Power to Decide What CALEA Compliance Means ..... 9

D. By Forcing Compliance to Begin Before Defining What Compliance Means, the Commission Had to Decide the Public Interest Test of the Substantial Replacement Provision without Knowing How Much Compliance Would Cost or What Its Impact Would Be on Privacy and Network Security..... 12

E. It Was Arbitrary and Capricious to Force Compliance to Begin While Leaving Large Unanswered Questions about Who Is Covered ..... 13

1. The Commission cast doubt on the scope of the private network exemption..... 13

2. Some entities will be exempt under 102(8)(C)(ii), but the Commission has not even set procedures for invoking the exemption..... 14

3. The Commission has indicated that some covered entities may not be required to comply “fully” ..... 14

**II. MOVANTS ARE LIKELY TO SUCCEED ON THE UNDERLYING MERITS OF THEIR APPEAL**..... **15**

A. The CALEA Statute Plainly Exempts Information Services, and the Commission Has No Authority to Alter or Ignore that Exemption. .... 15

B. The Commission’s Construction and Application of the “Substantial Replacement Provision” Is Squarely Contrary to the CALEA Statutory Language..... 16

**III. THE EQUITIES STRONGLY FAVOR A STAY. .... 17**

A. By Imposing a Compliance Deadline But Deferring Decision on What Compliance Means and Who May be Exempt, the Commission Has Forced Entities to Expend Resources Developing Surveillance Features That May Ultimately Not Be Required ..... 17

B. No Other Parties Will Be Harmed if a Stay Is Issued ..... 18

C. With No Evidence whatsoever that the Government Has Been Unable to Intercept Internet Communications, and With Assurances of Continued Cooperation from all Service providers, The Public Interest Will Not be Harmed by a Stay ..... 18

**CONCLUSION ..... 20**

## SUMMARY

This Request for a Stay seeks both a stay of the Commission's First Report & Order pending the release by the Commission of the subsequent orders anticipated by that first Order, and a stay of the First Report & Order pending review of that Order by the U.S. Court of Appeals for the District of Columbia Circuit.

The bifurcated approach the Commission adopted in this proceeding – declaring in general terms that new entities were covered by CALEA and immediately setting a deadline for “full compliance,” but deferring to later orders both the question of what compliance means and the resolution of possible exemptions from coverage – has raised a host of questions and put many entities in the impossible position of beginning compliance efforts without knowing what is required and whether they are even covered. In retrospect, it was clearly unreasonable, arbitrary and capricious, and not in accordance with law for the Commission to set a compliance deadline without answering basic questions about what compliance requires and who exactly is covered.

The unanswered threshold questions include those the Commission expressly raised in the First Report and Order about “CALEA lite” and the scope of CALEA's section 102(8)(C)(ii) exemption, as well as critical questions still unresolved from the first NPRM about what is “call-identifying information” on a broadband connection (on which even the FBI has not offered an opinion on the record).

Not only did the Commission order compliance efforts to begin without saying what compliance means, it is becoming increasingly clear that the Commission's articulation of its decision as to who is covered has caused confusion and uncertainty. Footnote 100, broadly read, would effectively eliminate the private network exemption. The Commission may yet reasonably clarify where it draws the line between exempted private networks and covered

public networks, but the pressure caused by the impending “full compliance” deadline, and the prospect of \$10,000 a day fines in 18 months, is such that private networks would feel compelled by the deadline to begin taking measures to comply even if they will later be found to be exempt.

The way the Commission structured this process, it has unreasonably, arbitrarily and capriciously put entities in an impossible position, forcing them to spend resources on compliance that may later be ruled to have been unnecessary or adopting compliance measures that may later be deemed to be insufficient, forcing retrofitting. That is the essence of irreparable harm. To avoid such harm, the Commission should stay its First Report and Order.

Beyond the enormous difficulties caused by the Commission’s bifurcated approach, there are substantial legal arguments challenging the Commission’s statutory authority to extend CALEA to information services, and about the Commission’s interpretation of the “substantial replacement provision.” Although the Commission rejected challenges to its authority and interpretation, those challenges are substantial (and in the view of the undersigned, meritorious). The First Report and Order imposes a sweeping and potentially costly new regulatory regime on an entire segment of industry that previously has been largely unregulated (including previously unregulated educational institutional and other non-profit entities), and the full scope of the costs and burdens to be imposed on the Internet has not yet even been determined. In light of the substantial questions about the underpinnings of the First Report and Order, the Commission should stay the order pending judicial review of those questions.

Public interest values all weigh in favor of a stay. Most especially, it is important to note that DOJ/FBI *never* identified *any* instance or circumstance in which law enforcement has been unable to intercept a target’s Internet communications. Thus, it is clear that there is *not* a critical need that requires compliance to begin immediately.

For these reasons, the undersigned entities respectfully move the Federal Communications Commission for a stay of the entire First Report and Order pending resolution of the appeals of the First Report and Order, or at a minimum a stay of the compliance deadline in its First Report and Order until such time that the Commission: (1) following comment by DOJ/FBI and replies by affected parties, has ruled what CALEA “requirements mean in a broadband environment,” including which entities in a decentralized network are responsible for which capabilities; (2) has reaffirmed the private network exemption; (3) has decided whether some entities are subject only to “CALEA lite;” and (4) has set procedures for section 108(8)(C)(ii) exemptions.

If this stay request is not granted by December 7, 2005, however, the undersigned will seek a stay from the D.C. Circuit.

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

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

**REQUEST FOR STAY PENDING ISSUANCE OF SUBSEQUENT ORDERS  
AND FOR STAY PENDING JUDICIAL REVIEW**

**SUBMITTED ON BEHALF OF**

**CENTER FOR DEMOCRACY & TECHNOLOGY, AMERICAN LIBRARY  
ASSOCIATION, ASSOCIATION FOR COMMUNITY NETWORKING, ASSOCIATION  
OF COLLEGE AND RESEARCH LIBRARIES, ASSOCIATION OF RESEARCH  
LIBRARIES, CHAMPAIGN URBANA COMMUNITY WIRELESS NETWORK,  
ELECTRONIC FRONTIER FOUNDATION, ELECTRONIC PRIVACY  
INFORMATION CENTER, PULVER.COM, SUN MICROSYSTEMS and TEXAS  
INTERNET SERVICE PROVIDERS ASSOCIATION**

Movants respectfully request that the Commission stay the effectiveness of its First Report and Order,<sup>1</sup> for two independent reasons. First, it was arbitrary and capricious to set an 18 month deadline requiring previously unregulated Internet companies and non-profit institutions to begin redesigning their networks and services to facilitate government wiretapping while leaving those entities uncertain as to whether they would actually be covered and guessing as to what compliance actually requires. Faced with \$10,000 a day fines 18 months from now, movants are being forced to begin immediately to expend resources that they will have lost irreparably if it is later determined that they were not required to comply at all or that the

---

<sup>1</sup> First Report and Order and Further Notice of Proposed Rulemaking, *In the Matter of Communications Assistance for Law Enforcement Act*, ET Docket No. 04-295, RM-10865, FCC 05-153 (released Sep. 23, 2005), published 70 Fed. Reg. 59664 (Oct. 13, 2005).

compliance method they chose did not meet the capability requirements of the CALEA as later interpreted by the Commission.

Second and in addition, because this matter poses substantial questions of first impression about the Commission's statutory authority to extend CALEA to the Internet – questions that individual Commissioners have acknowledged must be resolved in the courts or by Congress – movants seek a stay pending review of the order by the U.S. Court of Appeals for the D.C. Circuit.

While movants face an irreparable loss if a stay is not granted, no harm will fall to national security or law enforcement, since the record is clear that government agencies are already able to intercept Internet communications. Nor will a stay have any impact on voluntary efforts, which commenters uniformly stated were ongoing and would continue without a CALEA mandate.

If the Commission were to grant the stay requested here, the undersigned would join the Commission in a request to the Court of Appeals for an expedited review of the First Report and Order.

## **BACKGROUND**

In March 2004, the Department of Justice, the Federal Bureau of Investigation, and the Drug Enforcement Agency (“DOJ/FBI”) filed a petition asking the Commission to extend the Communications Assistance for Law Enforcement Act (“CALEA”)<sup>2</sup> to the Internet. Entities covered by CALEA must design their networks and services to be easily monitored by the government. Passed in 1994, the Act by its terms applies only to telecommunications common carriers. In response to the DOJ/FBI petition and following comments, the Commission issued a

---

<sup>2</sup> Pub. L. No. 103-414, 108 Stat. 4279 (1994), codified as 47 U.S.C. §§ 1001-10 and 47 U.S.C. § 229.

Notice of Proposed Rulemaking. After further comments, on August 5, 2005, the Commission announced its determination to extend CALEA to facilities-based broadband Internet access providers and providers of interconnected Voice over Internet Protocol (“VoIP”) service. The Commission released the text of its decision as the First Report and Order (“Order” or “First R&O”) on September 23, 2005. The order was summarized in the Federal Register on October 13, 2005, and by its terms became effective on November 14, 2005.<sup>3</sup>

In its Order, the Commission imposed a compliance deadline of 18 months following the effective date of the Order, requiring that by such time “newly covered entities and providers of newly covered services must be in full compliance” with CALEA. First R&O ¶ 46. Under CALEA, non-compliant entities face \$10,000 a day fines. *See* 18 U.S.C. § 2522(c)(1).

At the same time, however, the Commission expressly deferred deciding and defining what “full compliance” with CALEA means. As the Commission acknowledged:

Our action in this Order is limited to establishing that CALEA applies to facilities-based broadband Internet access providers and interconnected VoIP service providers. The Notice raised important questions regarding the ability of broadband Internet access providers and VoIP providers to provide all of the capabilities that are required by section 103 of CALEA, *including what those capability requirements mean in a broadband environment*. The Notice also sought comment on a variety of issues relating to identification of future services and entities subject to CALEA, compliance extensions, cost recovery, and enforcement. We will address all of these matters in a future order.

First R&O ¶ 46 (emphasis added) (footnotes omitted).

The Commission based its extension of CALEA to Internet on three new constructions of the CALEA statutory language. First, the Commission decided that CALEA’s blanket exemption of “information services” did not exempt broadband access or VoIP services (which

---

<sup>3</sup> The Order states that it becomes effective 30 days after its publication in the Federal Register, which occurred on October 13, 2005. *See* First Report and Order ¶ 62. The thirtieth day fell on a weekend, and thus the Order was effective on November 14, 2005, and compliance with the Order is required by May 14, 2007.

the Commission has ruled are information services in all other contexts where it has acted). Second, the Commission decided that CALEA's "substantial replacement" language (a) should be interpreted as a "functional" test rather than a market-based test and (b) can be applied to an entire industry instead of to particular entities. Third, the Commission decided that it could rule on the public interest standard in the substantial replacement test without considering the cost, privacy, or network security implications of forcing CALEA compliance on Internet services.

### **REASONS FOR A STAY**

Section I below seeks a stay pending further Commission proceedings. This Section focuses on only one element of the First Report and Order: the Commission's decision to set a deadline for "full compliance" without defining what compliance means and while leaving open questions about who is covered. *See* First R&O ¶ 46. Section II below seeks a stay pending appeal.

When reviewing stay motions, the Commission follows the standards articulated by the D.C. Circuit, granting stays when 1) the movant is likely to prevail on the merits; 2) the movant will likely suffer irreparable harm absent a stay; 3) others will not be harmed if a stay is issued; and 4) the public interest will not be harmed. *See In re Virgin Islands Telephone Corp.*, 7 FCC Rec. 4235 (Jun.19, 1992), at ¶ 13; *Washington Metro. Area Transit Comm'n v. Holiday Tours, Inc.*, 559 F.2d 841, 842-43 (D.C. Cir. 1977).

In this proceeding, a stay of the compliance deadline is strongly justified on all prongs of this test. Regardless of how questions of CALEA's application to the Internet are resolved by the Court of Appeals, movants are likely to succeed before the Court of Appeals on their argument that (as should be clear to the Commission) it was arbitrary and capricious for the Commission (1) to require entities to begin complying before telling them how to comply; and

(2) to require entities to begin complying before some of them could clarify whether they were covered or not. It is also clear that movants face irreparable harm if a stay is not granted, that a stay will harm no other parties, and that the public interest will not be harmed. Voluntary compliance efforts will continue under a stay, and industry-government discussions on what compliance means can also go forward. The public interest in national security and law enforcement will not be harmed, since there is no evidence that government agencies are unable to intercept Internet communications, and other aspects of the public interest – avoidance of unnecessary expenditures, identification and mitigation of the effects of CALEA compliance on privacy and network security – will be served by a stay.

The request for a stay pending appeal is similarly strong. As at least two Commissioners appear to recognize,<sup>4</sup> the appeals raise substantial legal questions about the statutory authority of the Commission to extend CALEA, and we believe there is a strong likelihood of success the merits. In light of the equities discussed above, the Commission should grant a stay pending appeal.

**I. IT WAS ARBITRARY AND CAPRICIOUS TO FORCE ENTITIES TO BEGIN COMPLYING WHILE DEFERRING TO AN UNCERTAIN FUTURE DATE DECISIONS AS TO WHAT “COMPLIANCE” MEANS, WHO EXACTLY IS COVERED, AND WHO IS ENTITLED TO AN EXEMPTION.**

The undersigned believe that they are likely to succeed before the Court of Appeals on their argument that, as a matter of statutory interpretation, the Commission had no authority under CALEA to regulate the Internet or Internet applications. However, even assuming that the Commission was correct in its interpretation of CALEA’s coverage, the decision of the Commission to set a “full compliance” deadline but then confuse the question of who was

---

<sup>4</sup> See First R&O (statements of Commissioners Abernathy and Copps).

covered and withhold a clear statement of what an entity must do to comply was arbitrary and capricious on a number of levels. As the Commission has done in other cases,<sup>5</sup> it should stay the effective date of its First Report and Order until the enormous uncertainty about the Order is resolved.

The need for a stay is reinforced by the reconsideration petition filed by the United States Telecom Association. Even though some of USTA's members strongly supported the extension of CALEA to the Internet, USTA has petitioned for reconsideration of the First R&O because the "Commission's decision to start the clock on November 14, 2005 (rather than on the effective date of its forthcoming capability order) places broadband and VoIP providers in an untenable position." USTA Petition (Nov. 14, 2005) at 2. USTA concludes:

Without answers to ... basic questions about the scope of their CALEA obligations, broadband and VoIP providers cannot reasonably be expected to become CALEA compliant within the existing 18-month timeframe established by the Commission." *Id.* at 3.

**A. The 18 Month Deadline, as the Average of Uninformed Estimates, is Itself Arbitrary and Capricious**

Without any decision as to what must be done to comply, the Commission had no way to determine rationally how long it would take to comply. Various parties, in their comments to the Commission, estimated how long it would take to comply if CALEA were extended to the Internet. The Commission seems to have picked 18 months as an average of what various parties said it would take to comply. *See* First R&O note 138. But the parties based those estimates on their *assumptions* about what compliance would entail. Until the Commission translates those

---

<sup>5</sup> *See, e.g.*, RULES AND REGULATIONS IMPLEMENTING THE TELEPHONE CONSUMER PROTECTION ACT OF 1991, Fax Ban Coalition Petition for Further Extension of Stay, FCC 05-132, CG Docket No. 02-278, 36 Comm. Reg. (P & F) 286 (adopted and released June 27, 2005).

assumptions into a ruling, the commenters' estimates of compliance remain unfounded.

Averaging a series of uninformed estimates does not constitute reasoned decision-making.

Moreover, setting a single deadline for a wide range of entities was arbitrary and capricious. The DOJ/FBI have stated on the record, and the Commission itself has acknowledged, that compliance may mean different things for differently situated entities. *See* First R&O ¶ 44; Comments of the United States Department of Justice, at 44 (filed Nov. 8, 2004) ("DOJ Comments"). Depending on what DOJ/FBI demands for surveillance features the Commission grants, and depending on which entities within the Internet's decentralized architecture are responsible for which capabilities, "compliance" may require for some service providers a massive change in operations or even network architecture. For others, it may not. In these circumstances, to set a one-size-fits-all "full compliance" deadline for all newly covered entities and services was the epitome of arbitrariness and capriciousness.

#### **B. It is Arbitrary and Capricious to Require Entities to Begin Compliance Measures Without Telling Them What Compliance Means**

In the initial NPRM, the Commission acknowledged that it was unclear how CALEA's requirements would translate to the Internet. It sought comment on what key CALEA requirements like "call-identifying information" would mean in a broadband Internet context. Yet it ordered compliance without answering that question. This critical problem is exacerbated by the fact that – as far as the public record reflects – even DOJ/FBI themselves do not know what they will demand that newly covered entities do to "comply" with CALEA. In responding to the first NPRM, the DOJ/FBI said that it was too "ambitious" to say what CALEA meant for the Internet. *See* DOJ Comments, at 39-41. As recently as September 8, 2004, the FBI had *not yet decided* what it intends to demand in the way of call-identifying information, a key term that is likely to be the center of implementation controversies for the Internet as it was for the PSTN.

When pressed at a Congressional hearing on what would be involved with call-identifying information, Deputy Assistant Director of the FBI Marcus Thomas stated:

With regard to the call identifying information, which is really what you more seem to be pointing at . . . , I do not think that is an issue that has actually matured yet. I do not think anyone has a complete vision of how that will be carried out.<sup>6</sup>

Since September 8, 2004, at least as far as is reflected in the record in this proceeding, FBI/DOJ have failed to inform the Commission or the public what they believe CALEA compliance means in the Internet context.

The Commission compounded the uncertainty that movants face by suggesting in its Further Notice of Proposed Rulemaking (issued as part of the First R&O) the possibility of “CALEA lite.” The Commission stated, “In addition, we seek comment on the appropriateness of requiring something less than full CALEA compliance for certain classes or categories of providers, as well as the best way to impose different compliance standards.” First R&O ¶ 49. So not only has the Commission acknowledged that a uniform standard would be applied differently to differently situated entities that were required to achieve “full compliance,” but also there might be a category of entities for whom less than full compliance was required. It is fundamentally arbitrary and capricious to require, as the Commission did, that “*all*” providers of facilities-based broadband Internet access and interconnected VoIP must be “in full compliance” within 18 months, First R&O ¶ 46 & note 138, and then three paragraphs later seek comment on whether certain classes or categories of covered providers might be subject to “something less than full CALEA compliance.” *Id.* ¶ 49

That the Commission’s failure to define compliance is causing uncertainty and confusion in the marketplace is readily apparent from the comments filed on November 14, 2005, in

---

<sup>6</sup> Testimony of Marcus Thomas, Energy & Commerce Hearing, at 55.

response to the Commission's Further Notice of Proposed Rulemaking. In those comments, both large and small service providers expressed an inability to move forward without knowing what compliance means. For example, the Information Technology Industry Council (which represents many of the nation's leading information technology companies) commented that "the Commission has set a highly unrealistic compliance date of eighteen months from the effective date of its First Report and Order, even though the Commission failed to provide crucial guidance in that order as to the full extent of providers' obligations."<sup>7</sup> At the other end of the spectrum, a very small rural ISP submitted the following "brief comment" reading (in its entirety):

C&W Enterprises is a provider of broadband services to rural areas in Western Texas. While we would like to comply with any law enforcement agency in pursuing its interests, it is difficult to assess what the costs would be for our company or what type of exemption we would advocate without knowing what we will be required to do under the CALEA rules. Therefore, we request that the Commission pursue this issue in a future rulemaking once such requirements have been proposed or determined.<sup>8</sup>

Industry participants large and small simply have no idea what they are expected to do within the 18 month deadline set by the Commission.

**C. By Immediately Setting a Compliance Deadline, the Commission Arbitrarily and Capriciously Delegated to the FBI the Power to Decide What CALEA Compliance Means**

It was also unreasonable, arbitrary and capricious, and not in accordance with the statutory terms of CALEA, for the Commission to set a "full compliance" deadline and then defer to "discussions" between the FBI and "appropriate industry representatives" the resolution of questions about what compliance means. First R&O ¶ 46. The issues to be resolved are not

---

<sup>7</sup> Comments of the Information Technology Industry Council, filed Nov. 14, 2005, at 6 (footnotes omitted).

<sup>8</sup> Brief Comments of C&W Enterprises, filed Nov. 14, 2005.

technical issues that can be resolved by standards bodies. They are questions of responsibility and capability. It might have been appropriate for the Commission to seek industry views on what constitutes “call-identifying information” in the context of broadband access, but it should not have ordered compliance to begin while that question was outstanding.

Because the FBI can wield the threat of an enforcement action under section 108, the Commission has in effect delegated to the FBI the answering of questions the Commission left unanswered. With the looming deadline, the FBI can say in its “discussions” with industry representatives, “Define call-identifying information our way and you’ll be fine, define it a different way and we may bring a civil action against you for non-compliance in 18 months.” Faced with this threat, a company or non-profit entity would be unlikely to devote scarce resources to forms of compliance the FBI did not accept.<sup>9</sup> But if the Commission (as it did in culling through the FBI’s CALEA punchlist for the PSTN) eventually adopts a definition of “call-identifying information” that does not include all of the intercept features the FBI advances in its discussions with industry, the damage will be irreparable – entities will already have spent resources complying with the FBI’s punchlist.

In essence, the Commission, by forcing compliance to begin now, has delegated its rulemaking authority to the FBI. This de facto delegation of authority to the FBI to decide how CALEA will be complied with is directly contrary to the structure of CALEA, under which

---

<sup>9</sup> The First R&O creates a situation even worse than what happened in the process of applying CALEA to the PSTN. There, as the relatively homogeneous telephone industry tried to develop a standard to implement CALEA, the FBI issued detailed “requirements” documents defining very precise features it wanted built into communications equipment and architectures. The FBI told carriers that it would challenge as deficient any standard that did not include all its stated “requirements.” Carriers and their equipment manufacturers were eager to take advantage of CALEA's safe harbor provision, so they incorporated many of the FBI's design features, even ones the carriers believed were not required by CALEA. (Despite that cooperation, the FBI still brought a deficiency proceeding, to get some additional items.)

industry bodies were supposed to develop compliance standards, in consultation with the government, but not under the control of the government. Under CALEA, if the government or anyone else considered an industry standard to be deficient, a petition could be filed at the Commission. *See* 47 U.S.C. § 1006(b). Conversely, if no standard was developed, anyone could petition the Commission to establish one, in order to get its safe harbor protection. The 18 month deadline, however, fundamentally shifts the balance of power under the statutory structure, giving the FBI effective control of the definition of compliance, because covered entities cannot develop a full safe harbor standard, resist FBI demands and risk a deficiency proceeding within the next 18 months. The cost exposure is too great. Nor is there any assurance that the Commission, having failed so far to define what CALEA requires, could develop a standard in sufficient time, even if someone petitioned for the lack of one. Hence the shift of design power to the FBI.

Given the way the Commission has structured its approach to CALEA, a possible outcome is that there will be no safe harbor standard as such for broadband access and VoIP. In the absence of a standard, all enforcement is in the hands of the FBI, and the mere threat of a lawsuit under CALEA section 108 and 18 U.S.C. § 2522 will be enough to force covered entities to go along with the FBI's demands. It was arbitrary and capricious for the Commission to structure compliance in this way; having overridden the statute and taken on the Internet, the Commission should have gone finished the job and defined what compliance means.

**D. By Forcing Compliance to Begin Before Defining What Compliance Means, the Commission Had to Decide the Public Interest Test of the Substantial Replacement Provision without Knowing How Much Compliance Would Cost or What Its Impact Would Be on Privacy and Network Security**

The Commission decision to mandate compliance without deciding what compliance means had further implications that render the Commission's approach arbitrary and capricious. The substantial replacement test requires the Commission to weigh cost and other factors against the public interest in national security and law enforcement. Even assuming that there was evidence of the government's failure to intercept Internet communications (in fact there was none), the Commission should have weighed those law enforcement and national security interests against the costs of compliance. It did not perform such a weighing of concerns, however, because it could not determine the cost of compliance without determining what compliance meant.

Similarly, the Commission should have considered the impact of its order on privacy. Privacy was one of Congress' key concerns in enacting CALEA. *See* 47 U.S.C. § 1006(b)(ii). Again, the Commission's public interest determination did not evaluate the privacy implications of extending CALEA to the Internet, because the Commission never decided what compliance meant.

Likewise, the Commission never even mentioned the impact of CALEA compliance on network security. It is widely recognized that the Internet is fraught with security vulnerabilities. Computer experts have argued that CALEA compliance could weaken the communications infrastructure. The Commission gave no attention to this issue in its public interest determination, and could not until it decided what compliance entailed.

## **E. It Was Arbitrary and Capricious to Force Compliance to Begin While Leaving Large Unanswered Questions about Who Is Covered**

Despite its best efforts, the Commission failed in the First Report and Order to clarify who is covered by CALEA.<sup>10</sup> Especially among universities and libraries, but also among other operators of private networks, the confusion generated by the First R&O brings pressure on entities to begin compliance even if they are later exempted.

### **1. The Commission cast doubt on the scope of the private network exemption**

The First R&O, for example, has generated significant uncertainty about whether “private networks” (exempted under 47 U.S.C. § 1002(b)(2)(B)) will in fact be exempt from CALEA if those networks “are interconnected with . . . either the PSTN or the Internet.” First R&O at note 100. Since there exist very few advanced networks that are wholly *unconnected* from the Internet, the Commission’s analysis could be read to indicate that the vast majority of otherwise private networks are nevertheless covered by CALEA. Moreover, if the Commission believes that such networks are covered, then the time for compliance has already started to run.

The combined uncertainty and running deadline create an untenable situation for network operators.<sup>11</sup> Numerous entities – ranging from the Telecommunications Industry Association to

---

<sup>10</sup> See Roy Mark, “FCC Rings New Round of Regulatory Uncertainty,” September 28, 2005, internetnews.com <http://www.internetnews.com/bus-news/article.php/3551911>; Declan McCullagh, “Perspective: Fahrenheit FBI,” August 9, 2004, cNet [http://news.com.com/Fahrenheit+FBI/2010-7352\\_3-5300198.html](http://news.com.com/Fahrenheit+FBI/2010-7352_3-5300198.html) (“A new U.S. government decision extending wiretapping regulations to the Internet raises far more questions than it answers.”); Scott Bradner, “Still more questions about the FCC order on 'Net wiretapping,” Network World, October 17, 2005 <http://www.networkworld.com/columnists/2005/101705bradner.html>; Scott Bradner, “Internet wiretapping: More questions than answers,” Network World, October 10, 2005, <http://www.networkworld.com/columnists/2005/101005bradner.html>.

<sup>11</sup> This uncertainty is particularly problematic for innovators creating new types of networks. For example, the Champaign Urbana Community Wireless Network (CUWN) is a mesh “wireless cloud” that is primarily designed to facilitate sharing of local content. While CUWN buys a commercial DSL line to provide connection to the broader Internet cloud, it primarily provides to users customer premise equipment (a “node”) which meshes with other nodes within range. While CUWN may help to maintain these nodes, the actual node belongs to the customer and may or may not be used to provide access to the broader Internet. If the Commission is effectively reading the private network exemption out of the CALEA statute (as it did with the information services exemption), there is significant uncertainty as to how mesh networks should or could be covered by CALEA.

libraries to individual colleges and universities – raised the uncertainty caused by the Commission’s order.<sup>12</sup> It is arbitrary and capricious for the Commission to simultaneously cast doubt on another clear exclusion from CALEA while at the same time starting the compliance clock ticking.

**2. Some entities will be exempt under 102(8)(C)(ii), but the Commission has not even set procedures for invoking the exemption**

Ignoring the requirement that it identify a specific “person or entity” whose service has become a “replacement for a substantial portion of the local exchange service,” the Commission turned the statute on its head and said that specific persons or entities offering broadband Internet access or VoIP services who believe that they should be exempt must show that they have not become a replacement for substantial part of local exchange. Yet the Commission has not even set procedures for applying for exemptions under 102(8)(C)(ii). Until such procedures are created, the Commission should stay its Order.

**3. The Commission has indicated that some covered entities may not be required to comply “fully”**

It was arbitrary and capricious for the Commission to start the compliance clock ticking while also seeking comments on the appropriateness of requiring something less than full CALEA compliance for certain classes or categories of providers. The Commission apparently contemplates a three step process: first, decide whether it is appropriate to require something less than full CALEA compliance; second, decide which *classes or categories* of service providers would be eligible for “CALEA lite;” third, conduct a process for those who believe they fit within one of the categories to apply and find out if they qualify for CALEA lite. Under the 18

---

<sup>12</sup> See, e.g., Comments of the Telecommunications Industry Association, filed Nov. 14, 2005, at 4; Comments of the American Library Association, Association of Research Libraries and Association of College and Research Libraries, filed Nov. 14, 2005, at 5; Comments of Duke University, filed Nov. 14, 2005, at 2.

month deadline for “full compliance,” entities who would be subject to less than full compliance under this process must still expend resources on full compliance while this lengthy CALEA lite process moves forward, for no entity can determine now whether it will be exempt under a undefined process. It is arbitrary and capricious for the Commission to launch a “CALEA lite” process and then force entities seeking to invoke the process to undergo the double expense of applying for “CALEA lite” status and immediately beginning full CALEA compliance.

## **II. MOVANTS ARE LIKELY TO SUCCEED ON THE UNDERLYING MERITS OF THEIR APPEAL.**

The undersigned and others have exhaustively detailed the grounds of which the Commission lacks the authority to extend CALEA as it did.<sup>13</sup> Among the grounds are:

### **A. The CALEA Statute Plainly Exempts Information Services, and the Commission Has No Authority to Alter or Ignore that Exemption.**

Although the First Report and Order asserts (at ¶ 9) that CALEA’s statutory language is ambiguous and thus must be interpreted by the Commission (in an attempt to move the statutory analysis into the second prong of “Chevron”), the exclusion of “information services” – included by Congress in two different places in the statute – could not be more clear. Contrary to the Commission’s assertion (at ¶ 19), the exclusion of information services from CALEA does not create any “irreconcilable tension” that the Commission must interpret the statute to resolve.

The exclusion of information services have been extensively briefed in prior comments to the Commission, and the undersigned incorporate their prior comments into this request for a stay. The logic used by the Commission in its First Report and Order is circular and self-fulfilling, and wholly reads the information services exclusion out of the statute. It is undeniable

---

<sup>13</sup> The arguments raised in the undersigned’s prior comments in the rulemaking are incorporated herein. *See* Joint Comments of Industry and Public Interest, filed Nov. 8, 2004; Joint Reply Comments of Industry and Public Interest, filed Dec. 21, 2004.

that CALEA clearly includes telecommunications carriers and clearly excludes information services. What the Commission's First Report and Order does, however, is to declare with no foundation that anything it deems to be included within the category of "telecommunications carriers" must by definition *not* fall into the category of "information services." This reasoning has no foundation in the statute, and as detailed extensively in prior comments the result reached by the Commission is directly contrary to the overwhelming legislative history indicating that Internet access is flatly excluded from CALEA.

**B. The Commission's Construction and Application of the "Substantial Replacement Provision" Is Squarely Contrary to the CALEA Statutory Language.**

As has been extensively briefed in prior comments, the "substantial replacement provision" in Section 1001(8)(B)(ii) does not support an extension of CALEA based on the current record. Again, the undersigned incorporate their prior comments on this point into this request for a stay.

The First Report and Order misconstrues the statute in at least three ways. First, the "functional" approach adopted by the Commission is contrary to the statutory language and clear congressional intent. Second, the Commission ignores the requirement that it identify a specific "person or entity" whose service has become a "replacement for a substantial portion of the local exchange service." Finally, the First R&O distorts the meaning of the phrase "switching and transmission services."

Even if the Commission's construction of the substantial replacement provision is correct, its application of that provision is flawed. There is no evidence in the record that any entity has become a substantial replacement for local service. Moreover, the factual record is wholly inadequate to support the public interest determination that is required by the statute. The record

lacks any evidence that there is a problem that needs to be addressed, as well as any evidence of what law enforcement intends to demand of newly covered entities.

### **III. THE EQUITIES STRONGLY FAVOR A STAY.**

Taken together, the three equitable prongs of the D.C. Circuit's standard provide strong support for a stay: (1) the movants will likely suffer irreparable harm absent a stay; (2) others will not be harmed if a stay is issued; and (3) the public interest will not be harmed. In the face of significant costs that service providers will have to begin incurring immediately, neither the Commission nor DOJ/FBI have yet to identify *any* instance where the government has to date been unable to intercept Internet communications pursuant to a lawful court order.

#### **A. By Imposing a Compliance Deadline But Deferring Decision on What Compliance Means and Who May be Exempt, the Commission Has Forced Entities to Expend Resources Developing Surveillance Features That May Ultimately Not Be Required**

The way the Commission structured this process, it has unreasonably, arbitrarily and capriciously put entities in an impossible position, forcing them to spend resources on compliance that may later be ruled to have been unnecessary or adopting compliance measures that may later be deemed to be insufficient, forcing retrofitting. That is the essence of irreparable harm.

The Commission has imposed an undeniable financial burden on a vast array of Internet and application service providers. Service providers will be required immediately to begin to restructure their service offerings and their networks, and they will irreparably lose the value of those expenditures when the Commission later determines what CALEA compliance means. This constitutes irreparable harm.

More broadly, the Commission's order has left a cloud looming over innovative new services that are in development, and there will be no way to erase the effect of that cloud following a reversal of the Commission's order. Thus, the public interest will be irreparably harmed in the absence of a stay.

**B. No Other Parties Will Be Harmed if a Stay Is Issued**

A stay will not harm those companies that are voluntarily complying with CALEA. It will not prevent discussions between industry and law enforcement "as they work together to develop capability solutions," which the Commission wants to encourage. As the Commission noted, even before this proceeding, industry was voluntarily working on compliance solutions. Likewise, as detailed below, law enforcement and national security agencies will not be harmed.

**C. With No Evidence Whatsoever that the Government Has Been Unable to Intercept Internet Communications, and With Assurances of Continued Cooperation from all Service providers, The Public Interest Will Not be Harmed by a Stay**

In five separate filings with the Commission, the DOJ/FBI and supporting law enforcement agencies completely failed to provide to the Commission evidence that law enforcement agencies have encountered *any* problem in intercepting Internet communications. In their initial petition to the Commission, in two rounds of comments on the petition, and two rounds of comments on the Notice of Proposed Rulemaking, the DOJ/FBI provided absolutely *no* evidence that they are unable to intercept Internet communications.

In the absence of any evidence of real – as opposed to hypothetical – problems, no credible arguments can be made that investigative efforts will be harmed by the granting of a stay. Other aspects of the public interest – avoidance of unnecessary expenditures, identification

and mitigation of the effects of CALEA compliance on privacy and network security – will be positively served by a stay.

There is also a strong public interest value in staying the First R&O because the impact of the extension of CALEA will fall disproportionately onto small ISPs, wireless ISPs (WISPs), and community wireless networks (CWNs). These small businesses cannot hope to comply immediately with the Commission's CALEA order without significant expense and disruption. The harm is further aggravated because these WISPs and CWNs often serve small businesses that cannot tolerate disruption in email or VOIP service. In many cases, WISPs and CWNs serve rural areas or neighborhoods underserved by other broadband providers. As a consequence, no alternate provider may exist to service the customers if CALEA mandates (mandates that may ultimately be reversed by the court or subject to exceptions relevant to these entities) disrupt service or force the networks to shut down.

Indeed, CWN and WISP services are playing important roles in providing connectivity for those displaced by Katrina, Rita, Wilma and other disasters. These vital services may be disrupted or delayed if those constructing ad hoc wireless networks using license exempt spectrum find themselves suddenly subject to CALEA mandates. As such networks may provide the only replacement for damaged or destroyed infrastructure, the public interest weighs heavily toward facilitating deployment rather than imposing new burdens.

Because of the great uncertainty created by the First R&O, and the significant possibility that the Order will be overturned on appeal, the public interest strongly supports a stay of the First R&O.

## CONCLUSION

For the foregoing reasons, the Commission should grant a stay of the compliance deadline announced in ¶ 46 of the First Report and Order, and should grant a stay pending appeal. If at least one of these stay requests is not granted by December 7, 2005, however, the undersigned intend to seek a stay from the D.C. Circuit.

ON BEHALF OF

CENTER FOR DEMOCRACY & TECHNOLOGY  
AMERICAN LIBRARY ASSOCIATION  
ASSOCIATION OF COLLEGE AND RESEARCH LIBRARIES,  
ASSOCIATION OF RESEARCH LIBRARIES  
ASSOCIATION FOR COMMUNITY NETWORKING  
CHAMPAIGN URBANA COMMUNITY WIRELESS NETWORK  
ELECTRONIC FRONTIER FOUNDATION  
ELECTRONIC PRIVACY INFORMATION CENTER  
PULVER.COM  
SUN MICROSYSTEMS and  
TEXAS INTERNET SERVICE PROVIDERS ASSOCIATION

Respectfully submitted by,

/s/

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

Albert Gidari  
Perkins Coie LLP  
1201 Third Avenue, Suite 4800  
Seattle, Washington 98101  
(206) 359-8688  
Counsel for American Library Association,  
Association of College and Research  
Libraries, and Association of Research  
Libraries  
(counsel continued on following page)

Andrew J. Schwartzman  
Harold Feld  
Media Access Project  
1625 K Street NW, Suite 1000  
Washington, DC 20006  
(202) 232-4300  
Counsel for Association For Community  
Networking, Champaign Urbana  
Community Wireless Network, and  
Texas Internet Service Providers  
Association

Lee Tien  
Kurt B. Opsahl  
Electronic Frontier Foundation  
454 Shotwell Street  
San Francisco, CA 94110  
(415) 436-9333  
Counsel for Electronic Frontier Foundation

Marc Rotenberg  
Sherwin Siy (admission pending in Calif.)  
Electronic Privacy Information Center  
1718 Connecticut Ave. NW, Suite 200  
Washington, DC 20009  
(202) 483-1140  
Counsel for Electronic Privacy  
Information Center

Jonathan Askin  
General Counsel  
pulver.com  
115 Broadhollow Road, Suite 225  
Melville, NY 11747  
(631) 961-1049  
Counsel for pulver.com

Dated: November 23, 2005