

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

In the Matter of)	
)	
Joint Petition for Rulemaking to Resolve)	RM-10865
Various Outstanding Issues Concerning the)	
Implementation of the Communications)	
Assistance for Law Enforcement Act)	

**COMMENTS OF THE
CENTER FOR DEMOCRACY & TECHNOLOGY**

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

Dated: April 12, 2004

TABLE OF CONTENTS

SUMMARY **iii**

INTRODUCTION **1**

I. CONGRESS LIMITED CALEA TO TELECOMMUNICATIONS COMMON CARRIERS; IT IS UP TO CONGRESS TO EXPAND IT **5**

 A. Congress Excluded the Internet and Internet Services from CALEA..... 5

 B. Congress Focused Where It Understood Law Enforcement’s Need to Be: On Common Carriers Providing Last Mile Connectivity 9

II. THE FBI FAILS TO IDENTIFY A SINGLE “PERSON OR ENTITY” WHOSE SERVICE HAS BECOME A “REPLACEMENT FOR A SUBSTANTIAL PORTION OF THE LOCAL EXCHANGE SERVICE” **12**

III. CALEA IS ILL-SUITED TO THE INTERNET; THE INTERNET AND SERVICES OVER THE INTERNET SHOULD NOT BE REQUIRED TO LOOK LIKE THE PSTN AND POTS **15**

 A. There Is No Need for the Commission to Act to Cover Packet Technology Used by Telecommunications Common Carriers for Other than Information Services – Packet Technologies Are Already Clearly Covered..... 16

 B. CALEA As Interpreted by the Commission Would Be a Nightmare for the Internet..... 17

 C. The Issue for Broadband, As It Was in Round One of CALEA Implementation, Would Be the FBI’s Desire to Pour Multiple Meanings into the Term “Call-Identifying Information” and to Expect Service Providers to Isolate and Format Call-Identifying Information on the Internet the Same Way It Is Treated in POTS 18

IV. DENYING THE FBI PETITION DOES NOT LEAVE THE INTERNET IMMUNE FROM SURVEILLANCE..... **19**

 A. VoIP Technology (and Internet Communications More Generally) Can be Tapped and Intercepted 20

 1. VoIP Services Provided by the Access Provider 22

 2. VoIP Services Provided by a Third Party Service Provider (with Call Content Passing Through the Third Party Network) 22

 3. VoIP Services Provided by a Third Party Service Provider (with Call Content Flowing Directly Between Calling Parties) 23

 4. Self-Provided VoIP Services (with no VoIP Service Provider) 23

B.	Internet Communications (including New Technologies) Can be Intercepted at the Access Provider, But Law Enforcement Must Move into the Twenty-First Century to Make Use of Such Interception.....	23
V.	LAW ENFORCEMENT’S APPROACH WOULD SEVERELY THREATEN INNOVATION IN THE UNITED STATES, AND WOULD CERTAINLY DRIVE INNOVATION OFF SHORE.....	25
A.	Law Enforcement’s Approach Would Roll Back the Development of Communications in the United States to Before the <i>Carterfone</i> Decision, which Fostered Innovation and the Advent of the Internet.....	25
B.	The Short History of the Internet is Full of Examples of Innovation Coming from Individual or Startup Efforts, and Such Innovation Would be Squelched by a Prior Authorization and Review Process.....	26
C.	Technology Innovation Would Be Driven Off Shore	28
VI.	THE FBI IS SEEKING TO REWRITE CALEA.....	28
A.	The FBI’s Pre-Approval Proposal would Shift Both the Burden of Going Forward and the Burden of Proof.....	29
B.	CALEA Already Has Clear Rules on Cost Allocation, Based on a Series of Factors That the FBI’s Petition Ignores	30
	CONCLUSION	31

SUMMARY

CDT recognizes and respects the substantial interests of law enforcement in carrying out surveillance on new communications technologies. However, contrary to the implications of the FBI's Joint Petition for Expedited Rulemaking (the "Petition"), broadband services are not untappable. So far there is no evidence that there is an interception problem whose solution would require the extension of CALEA to the Internet, a decision that in any case is up to Congress.

To the contrary, based on our understanding of the technology, law enforcement agencies currently have and in the foreseeable future will have the capability to intercept communications over broadband. The fact that CALEA does not reach the Internet does not mean the Internet is immune from law enforcement interception. Both the Internet in general, and broadband services in particular, can be intercepted. In some ways, Internet interception will be less convenient than PSTN interception; given the diversity of services, the information will come in different formats and law enforcement will have to work harder to determine what it is intercepting. In many cases, law enforcement agencies will have to decode call-identifying information themselves. In some situations, law enforcement will have to obtain call-identifying information from an entity other than the one from which it obtains content. In other ways, however, Internet surveillance will be easier, in that the digital nature of communications makes them easier to analyze, store, manipulate and transfer. And Internet surveillance will certainly be more fruitful, with no need for design mandates, as more and more information moves online.

Fundamentally, the Petition asks the Commission to go beyond its statutory authority and re-write the CALEA statute. Congress specifically limited CALEA to telecommunications common carriers, and specifically excluded the Internet and applications that run on top of the

Internet from CALEA coverage. In CALEA, Congress decided to impose design mandates only on telecommunications common carriers, a group of already heavily regulated entities, whose networks were characterized by highly centralized switches made by a handful of manufacturers. As the FBI Director testified, “the legislation is narrowly focused on where the vast majority of our problems exist: the networks of common carriers, a segment of the industry which historically has been subject to regulation.”

In arguing that the Commission should expand CALEA coverage using the alternative “replacement” language, the FBI has failed to identify any “person or entity” that is a “replacement” for a substantial portion of the existing local telephone service.

Congress was careful in CALEA to avoid impeding the development and deployment of new services and technologies. The FBI proposal that all new communications technology be reviewed by the FCC and FBI violates this intent and contradicts the enforcement provisions of CALEA, which put the burden on the Attorney General of going forward with an enforcement petition against a non-compliant carrier and which gave the courts very clear guidance in the factors to be balanced in an enforcement proceeding. The radical pre-approval proposal of the FBI would have a drastic and harmful impact on technology innovation in this country. Many important technologies in use on the Internet today had their origins in small startup companies or individual innovators, and the ability of such startups and innovators to continue to work in the U.S. would be greatly hampered by the FBI’s proposed review and design mandate process.

Finally, the FBI should not be allowed to re-write the procedural and enforcement mechanisms that are built into the statute. If new procedures are warranted, the FBI should seek such changes from the U.S. Congress.

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

In the Matter of)	
)	
Joint Petition for Rulemaking to Resolve)	RM-10865
Various Outstanding Issues Concerning the)	
Implementation of the Communications)	
Assistance for Law Enforcement Act)	

**COMMENTS OF THE
CENTER FOR DEMOCRACY & TECHNOLOGY**

Pursuant to the Public Notice issued March 12, 2004, DA No. 04-700, the Center for Democracy & Technology (“CDT”) respectfully submits these comments on the Joint Petition for Expedited Rulemaking (the “Petition”) filed by the U.S. Department of Justice, the Federal Bureau of Investigation, and the Drug Enforcement Administration.

INTRODUCTION

The Joint Petition for Expedited Rulemaking primarily asks the Commission (a) to declare that providers of broadband Internet access and “broadband telephony” services are covered by the Communications Assistance for Law Enforcement Act (“CALEA”), Public Law 103-414, and (b) to create in contravention of CALEA a regulatory process under which new communications protocols, applications, or services must be reviewed and approved by the FCC

and FBI before they can be deployed. In both respects, and in others, the Petitioners are asking the Commission to rewrite CALEA.

CDT recognizes and respects the urgent and substantial interests of law enforcement in carrying out surveillance on new communications technologies. However, contrary to the implications of the Petition, broadband services are not untappable. So far there is no evidence that there is an interception problem whose solution would require the extension of CALEA to the Internet, a decision that in any case is up to Congress. To the contrary, based on our understanding of the technology, law enforcement agencies currently have and in the foreseeable future will have the capability to intercept communications over broadband. In some ways, interception will be less convenient, in that law enforcement will have to go to different entities to obtain content and call-identifying information. And given the diversity of services, the information will come in different formats and law enforcement will have to work harder to determine what it is intercepting. In many cases, law enforcement will have to decode call-identifying information themselves. In some ways, however, Internet surveillance will be easier, in that the digital nature of communications makes them easier to analyze, store, manipulate and transfer. And Internet surveillance will certainly be more fruitful, as more and more information moves online.

The Petition does not actually say how CALEA's requirements would translate to Internet services. This is a major flaw in the Petition, for some of CALEA's requirements, particularly the concept of isolating "call-identifying information," do not readily transfer to the Internet. However, we fear that the goal of the Petition is to force the diversity of services available over the Internet into a single format resembling the telephone network and to require

Internet access providers to perform surveillance assistance functions similar to those performed by local exchange carriers on the PSTN.

CALEA was adopted in 1994 in response to law enforcement concerns that wiretaps would be more difficult in digital telephone networks than they had been with the analog phone system. CALEA required “telecommunications common carriers” to design basic wiretap capabilities into their networks. This was an unprecedented and controversial step, with implications not only for law enforcement but also for competition, innovation and privacy. Congress acted cautiously. After rejecting broader proposals, it focused on one specific segment of the communications infrastructure – the already highly regulated common carriers providing local exchange service. That is where most intercept activity was carried out by law enforcement and where intercept problems were being encountered, as documented by extensive factual inquiry in the early 1990s. Focusing on common carriers involved a relatively small number of entities. The solutions could all be implemented in central office and MTSO switches, which were manufactured by a handful of switch makers.

The Internet is fundamentally different. As the Commission has stated, “[w]hereas the PSTN’s design is logically and physically hierarchical, utilizing highly centralized signaling intelligence to connect parties to a communication, IP network design is ‘flat,’ distributing network intelligence and permitting highly dynamic and flexible routing And whereas enhanced functionalities delivered via the PSTN typically must be created internally by the network operator and are often tied to a physical termination point, IP-enabled services can be created by users or third parties, providing innumerable opportunities for innovative offerings competing with one another over multiple platforms and accessible wherever the user might have access to an IP network.” *In the Matter of IP-Enabled Services*, Notice of Proposed Rulemaking,

WC Docket No. 04-36, 2004 FCC LEXIS 1252, at ¶ 4 (Mar. 10, 2004) (“*IP-Enabled Services NPRM*”).

Congress, while it could not have foreseen the full course of Internet development, was well aware in 1994 that it was fundamentally different from the PSTN. For that reason, and for all the other reasons that national policy has left the Internet largely unregulated, Congress excluded the Internet and Internet applications from the design mandates of CALEA

As it has been implemented, CALEA has proven to be a difficult statute, to say the least. The FBI admits as much in the second half of its petition, where it states that the CALEA implementation process “is not working.” Petition, at 38. *See also id.* at 34 (“implementation of CALEA for packet-mode technologies has been largely unsuccessful”); *id.* at 53 (“problems and delays”); *id.* at 55 (“seemingly endless cycle of extensions that have consistently plagued the CALEA compliance process”); *id.* at 58 (“problems and delays”); *id.* (“carriers continue to express uncertainty”); *id.* at 68 (“a growing number of law enforcement agencies have increasingly expressed concern”). Clearly, given all the problems the FBI complains about with regard to CALEA in the PSTN, the Commission should not venture to extend the statute to the diversity of the Internet. The approach taken by the Commission to implementing CALEA for the PSTN gave the FBI very precise design control over telephone switching software. The FBI was able to convince the Commission to mandate very specific features, including – at substantial cost to carriers – features that gave the government capabilities going beyond those that had been available in older phone systems. Thus CALEA was used to enhance rather than merely preserve government surveillance capabilities. The approach taken by the Commission in the first phase of CALEA implementation is completely unsuited to the diversity and rapid pace of change of the Internet. This approach applied to the Internet would be a disaster.

The FBI's petition lacks the kind of factual detail that would be necessary to conclude even whether there is a problem in the first place. The petition contains only a few introductory sentences asserting that there is a problem, Petition at 8-9, but it is not even clear whether those sentences pertain to broadband services or the covered services that the FBI claims have not been brought into compliance. Nor is it clear whether they arise from inherent features of the technology design or from failures of communication between law enforcement and service providers. Until such a record is developed, it is impossible to tell what the problem is, and how it should be fixed.

We urge the Commission to deny those portions of the Petition that ask that the Commission (a) extend the reach of CALEA to broadband Internet access, or to VoIP or other information services, (b) create a review process for future technology, or (c) create new procedures and enforcement mechanisms different from those already in the statute. In response to the Petition, the Commission should respectfully note both the importance of the issues the Petition raises and the unique aspects of the Internet that would be affected by the Petition, and then should defer to Congress, where this matter belongs.

I. CONGRESS LIMITED CALEA TO TELECOMMUNICATIONS COMMON CARRIERS; IT IS UP TO CONGRESS TO EXPAND IT

A. Congress Excluded the Internet and Internet Services from CALEA

In adopting CALEA, Congress took the unprecedented and extraordinary step of requiring certain providers of communications services to design their equipment to be wiretap-friendly. Congress wisely took this step incrementally, based on a considerable factual record. Congress did not cover the waterfront with CALEA, and it certainly did not venture to regulate the then-relatively new arena of the Internet. U.S. policy was at the time, and remains today, that the Internet, Internet access services and Internet applications should remain unregulated to

promote innovation. That policy has paid off, facilitating the unprecedented rise of the Internet as a mass communications medium. As this Commission recently explained, the Internet has “become one of the great drivers of consumer choice and benefit, technical innovation, and economic development in the United States in the last ten years,” and this has occurred “in an environment that is free of many of the regulatory obligations applied to telecommunications services and networks.” *IP-Enabled Services NPRM* ¶ 1. It would be folly for the FCC to abandon that policy without congressional action. It would also be illegal.

Congress used a belt and suspenders approach to make clear that CALEA was focused on the already heavily regulated telecommunications carriers at the local exchange level, and not on the Internet.¹ It both defined the “telecommunications carriers” to which CALEA applied such that the Internet was not implicated, and it excluded “information services” – shorthand in 1994 for the Internet – from CALEA obligations not once, but twice.

CALEA applies only to “telecommunications carriers,” defined as “a person or entity engaged in the transmission or switching of wire or electronic communications as a *common carrier* for hire.” 47 U.S.C. § 1001(8)(A) (emphasis added). By defining a covered telecommunications carrier first and foremost as a common carrier, Congress clearly signaled its intention to cover only traditional telephone companies operating under common carriage rules. By focusing on traditional common carriers, it just as clearly excluded Internet service providers and application service providers, which were plainly not subject to FCC common carriage regulation.

Congress also made its exclusion of Internet services and providers explicit, in two ways. First, under CALEA, the term “telecommunications carriers” does not apply to “persons or

¹ Congress also specified that CALEA does not cover interconnection facilities, private networks, PBXs, and encryption. 47 U.S.C. § 1002(b)(2), (3).

entities insofar as they are engaged in providing information services,” such as email and Internet access. 47 U.S.C. § 1001(8)(C)(i).² Thus, even common carriers are not covered to the extent they are providing information services. Only their transmission facilities, subject to common carrier obligations, are covered.

Second, Congress separately specified that CALEA as a whole does not cover information services. *See* 47 U.S.C. § 1002(b)(2); *see also United States Telecom Ass’n v. FCC*, 227 F.3d 450, 455 (D.C. Cir. 2000) (“CALEA does not cover ‘information services’ such as e-mail and internet access”); *Telecommunications Carrier Assistance to the Government*, H.R. Rep. 103-827(I), at 23 (Oct. 4, 1994) (“*House Report*”) (CALEA obligations “do not apply to information services, such as electronic mail services, or on-line services, such as Compuserve, Prodigy, America On-line or Mead Data, or Internet service providers”). This Commission, too, has found that information services “such as electronic mail providers and on-line service providers” are exempt from CALEA. *In the Matter of Communications Assistance for Law Enforcement Act*, Second Report and Order, 15 FCC Rcd 7105, at ¶ 26 (1999) (“*Second Report and Order*”).

This category of “information services” is an Internet-age description of the FCC’s longstanding distinction between “basic” and “enhanced” services. As this Commission explained just last month, while providers of “basic” transmission services have long been regulated as common carriers, providers of “enhanced” applications riding on top of those basic transmission services have not. *IP-Enabled Services NPRM* ¶ 25. Today’s information services, which offer “a capability for generating, storing, transforming, processing, retrieving, utilizing,

² CALEA uses what may seem at first to be an oddly incongruous formulation: It covers telecommunications common *carriers* and excludes information *services*. But this makes sense when one realizes that CALEA is focused on the PSTN. The key distinction in CALEA is not between “telecommunications services” and “information services”; rather, it is between telecommunications common carriers and everyone else.

or making available information via telecommunications,” 47 U.S.C. § 153(20) (Telecommunications Act of 1996); *id.* § 1001(6)(A) (CALEA), are yesterday’s enhanced services. *IP-Enabled Services NPRM* ¶¶ 26-27. Thus, applications riding on top of common carriers’ transport services – whether those applications are Internet access, email or VoIP, and whether they are provided by the common carrier or someone else – are information services and are not covered by CALEA. *Second Report & Order* ¶¶ 26-27.³

The FBI tries in its Petition to make a great deal of the difference between the definition of “telecommunications carrier” in CALEA and the definition of “telecommunications service” in the Telecommunications Act of 1996. It is not clear that any of the differences cited by the FBI are meaningful. If anything, it would seem that CALEA is narrower, since it applies to carriers, not services, suggesting that Congress was focusing on certain entities, namely the local exchange carriers. In any event, the differences between the definitions of CALEA and the 1996 Act all pale in comparison to the key concept in both pieces of legislation: “common carrier.” Both the 1996 Act and CALEA rely on the concept of the common carrier to define the entities to which they apply, demonstrating that Congress’ focus was on the public switched telephone network – not the Internet. Furthermore, both the 1996 Act and CALEA define “information services” in substantially the same way, plainly excluding Internet services and applications from their coverage. *Compare* 47 U.S.C. § 1001(6)(A) *with* 47 U.S.C. § 153(20). As the Commission noted in the CALEA Second Report & Order, the two definitions will produce the same results “in virtually all cases.” *Second Report & Order* ¶ 13.

³ The only exception is for “joint-use facilities” such as DSL, where the telecommunications service over the PSTN is inseparable from the information service of providing access to the Internet. *Second Report & Order* ¶ 27. However, other modes of access to the Internet that do not use the PSTN, such as cable and satellite, are not subject to CALEA because CALEA only covers telecommunications common carriers. To the extent the FBI seeks to impose any law enforcement interception obligations beyond the Title III wiretap laws on such entities, it must ask Congress to address the issue.

The distinction between information services and telecommunications carriers may or may not be relevant in today's world. It may or may not be disappearing as technology advances. But the distinction clearly meant something to Congress in 1994 (and 1996), and it is a distinction whose legal significance can be altered only by Congress.

**B. Congress Focused Where It Understood Law Enforcement's Need to Be:
On Common Carriers Providing Last Mile Connectivity**

Law enforcement needs may or may not have changed since 1994. The FBI has yet to provide specific information about any technological barriers it faces in intercepting Internet communications. *See* Section IV, below. But if the FBI has legitimate law enforcement concerns in that regard, it must ask Congress to address them.⁴ The factual record when CALEA was enacted focused solely on law enforcement needs with respect to the PSTN, where the FBI had identified concrete problems with interception. Congress rejected attempts to broaden CALEA's effects to anyone other than a common carrier providing transmission services. Indeed, it was the focus on the PSTN that allowed CALEA to pass at all. As then-FBI Director Louis Freeh testified at a joint congressional hearing on CALEA in 1994, a broader bill covering all communications service providers "was rejected out of hand." Joint Hearings before the Subcomm. on Tech. and the Law of the Senate Comm. on the Judiciary and the Subcomm. on Civil and Const'l Rights of the House Comm. on the Judiciary on H.R. 4922 and S. 2375, at 49 (Mar. 18 and Aug. 11, 1994) ("*Joint Hearings*").

In the early 1990s, as the FBI brought forth concerns that technological changes in the PSTN were impeding its wiretap capability, Congress insisted on having a factual basis for any legislative mandate. The FBI surveyed its field offices twice to identify specific instances in

⁴ At a minimum, it would be improper for this Commission to issue any declaratory ruling in response to the FBI's petition applying CALEA to the Internet without the benefit of a full factual record.

which law enforcement agencies were precluded due to technological impediments from fully implementing authorized electronic surveillance. That evidence was presented to Congress. Most significantly, perhaps, representatives of the telecommunications industry acknowledged that there were specific technological impediments to law enforcement interception. The phone companies and the FBI created an “Electronic Communications Service Provider Committee,” through which representatives of all the RBOCs met with law enforcement on a regular basis to identify problems and solutions. The committee created a series of “action teams.” Ultimately, the chairman of the committee, a vice president of one of the RBOCs, stated in a letter that “there is in fact a problem.” In addition, the General Accounting Office did a survey and testified before Congress, confirming that there were legitimate impediments posed by new and emerging technologies.

CALEA was based on this factual record, which focused on the PSTN. The legislative history confirms that Congress addressed only the architecture of the PSTN. As Congress explained, “[e]arlier digital telephony proposals covered all providers of electronic communications services That broad approach was not practical. Nor was it justified to meet any law enforcement need.” *House Report* at 18. Congress further emphasized that “[i]t is also important from a privacy standpoint to recognize that the scope of the legislation has been greatly narrowed. The only entities required to comply with the functional requirements are telecommunications common carriers, the components of the public switched network where law enforcement agencies have always served most of their surveillance orders.” *Id.* Likewise, then-FBI Director Freeh testified that “[t]he current legislative proposal focuses on where the problems are – within the networks of common carriers. Hence, all other types of service providers (computer networks, PBX operators, etc.) have been eliminated from coverage.” *Joint*

Hearings at 39; *see also id.* at 7 (“the legislation is narrowly focused on where the vast majority of our problems exist: the networks of common carriers, a segment of the industry which historically has been subject to regulation”); *id.* at 115 (“[T]he coverage of the legislation focused on common carriers – entities that historically have been subject to regulation. We have acknowledged, as have [congressional] subcommittees, that almost all of our electronic surveillance problems have occurred, and will continue to occur in the foreseeable future, in the networks and systems of common carriers. Therefore, this legislation does not unreasonably and unnecessarily call upon small private branch exchange (PBX) operators, pure computer networks, or private networks to alter their systems and networks.”).

Common carriers have to comply with CALEA with regard to the *transmission* of electronic communications over their networks, but that only reinforces that Congress focused CALEA solely on the transport of communications over the PSTN. In 1994, Congress found “that law enforcement will most likely intercept communications over the Internet at the same place it intercepts other electronic communications: at the carrier that provides access to the public switched network.” *House Report* at 24. Thus, for example, if a subscriber of local telephone service used the line for voice, fax and dial-up Internet access, the common carrier providing the local service had to comply with CALEA with regard to all those modes of communications. But that individual’s Internet service provider – even if the same entity as the telecommunications carrier – is not subject to CALEA with regard to the Internet access service or other Internet applications. Today, there is no question that more and more people are accessing the Internet over something other than the PSTN. But if that shift has made it difficult for the FBI to intercept Internet communications, it must make its case to Congress for new legislation; CALEA simply does not address it.

At the time CALEA was passed, it was clear that excluding the Internet from its coverage was key to its enactment. Director Freeh himself explained that in order “to narrow the focus of this [legislation] so we can get the greatest support by the Congress and the committees,” the FBI agreed to exclude some “portions of the industry” from CALEA, such as cable companies. He went on: “In a perfect world, they would be in there, but . . . the last time we were here [before Congress], we were told specifically that [our proposal] was too broad and it had to be narrowed and focused.” *Joint Hearings* at 49-50. This Commission cannot add what the FBI explicitly gave up so that Congress would impose interception requirements on the PSTN.

The FBI is seeking to rewrite CALEA to get what Congress “rejected out of hand” in 1994 – essentially a broadbrush requirement that all communications access and service providers be required to take the extraordinary step of engineering their products and services to make them wiretap-friendly. The FBI cannot rewrite CALEA, nor can this Commission. If CALEA is to be expanded, it is Congress who must take that step.

II. THE FBI FAILS TO IDENTIFY A SINGLE “PERSON OR ENTITY” WHOSE SERVICE HAS BECOME A “REPLACEMENT FOR A SUBSTANTIAL PORTION OF THE LOCAL EXCHANGE SERVICE”

In addition to common carriers, Congress recognized in CALEA the possibility of covering entities that, while not common carriers, had become a replacement for the local exchange service. CALEA defines covered telecommunications carriers to include:

a person or entity engaged in providing wire or electronic communication switching or transmission service to the extent that the Commission finds that such service is a replacement for a substantial portion of the local telephone exchange service and that it is in the public interest to deem such a person or entity to be a telecommunications carrier for purposes of this title.

47 U.S.C. § 1001(8)(B)(ii). The test requires the Commission to evaluate whether a *particular person or entity* is a telecommunications carrier based on whether it is providing a service that

has replaced a substantial portion *of the local exchange*.⁵ That means that to take advantage of this provision, the FBI would have to identify a company that, in a given local exchange, had replaced a substantial proportion of the traditional local telephone exchange service. This provision of CALEA requires the Commission to undertake a factual inquiry into a particular company at a particular geographic location.⁶

The FBI has not even attempted to argue that any particular broadband service or VoIP provider has “replaced” a substantial portion of any particular local telephone exchange service. Instead of focusing on a particular “person or entity,” as CALEA requires, the FBI attempts to sweep entire categories of services into this provision. But CALEA covers “carriers,” not services.⁷

Moreover, the FBI ignores the word “replacement” and asks the Commission to amend it to read “alternative.” There is no doubt that broadband offers an alternative path to the Internet and that many people have dropped their narrowband access to the Internet in favor of broadband access. But broadband is a replacement for a service that was never covered by CALEA in the first place: narrowband access to the Internet. A replacement for an uncovered service must be an uncovered service. The fact that broadband service supports more applications than the old service does not make it covered. In essence, the FBI wishes the statute referred not to an entity

⁵ Again, this demonstrates that Congress in CALEA was focused on wiretaps within the PSTN.

⁶ The legislative history confirms this geographic emphasis, noting that the FCC can deem an entity to be covered by CALEA if it “serves as a replacement for the local telephone service to a substantial portion of the public within a state.” *House Report* at 20-21. Such a fact-intensive inquiry cannot be undertaken without a complete record; thus, here too the FCC should not issue any declaratory ruling on this issue without developing a factual record.

⁷ For this same reason, any inquiry by this Commission into the “functional equivalence” or “substitutability” of VoIP services for traditional telephony services as a result of its *IP-Enabled Services NPRM* is not relevant to the “replacement” test under CALEA. *See IP-Enabled Services NPRM* ¶ 37.

providing a “replacement” for the local telephone exchange service, but rather to a service that is an “alternative” to narrowband Internet access.

In any event, broadband Internet access has not replaced the local exchange service in any local exchange. Specifically with regard to VoIP services, the FBI cannot plausibly argue that it has replaced a “substantial portion” of local telephone service anywhere in the United States. The largest VoIP provider has only 130,000 customers worldwide, compared to 182 million local access lines in the United States. This Commission has not yet found *any* service to be a replacement for the local exchange, in any context – not even wireless service, where 3 percent to 5 percent of users have substituted wireless service for their primary local exchange line. *See In the Matter of Review of the Section 251 Unbundling Obligations of Incumbent Local Exchange Carriers*, Triennial Review Order, 18 FCC Rcd 16978, at ¶ 445 (Aug. 21, 2003). If wireless services are not a replacement for the local exchange, then VoIP (which many U.S. consumers have never even heard of) cannot be.

Finally, this provision of CALEA also demands that the FCC undertake a public interest analysis before deeming any particular entity a telecommunications carrier for purposes of CALEA. Congress directed that “[a]s part of its determination whether the public interest is served by deeming a person or entity a telecommunications carrier for the purposes of [CALEA], the Commission shall consider whether such determination would promote competition, encourage the development of new technologies, and protect public safety and national security.” *House Report* at 21. Thus, while legitimate law enforcement interests certainly play a role in any public interest analysis, so too do innovation and network security, which as discussed below will suffer if Internet and VoIP services are subjected to the strict regulatory requirements of CALEA.

In sum, the FCC has no statutory authority to expand the scope of CALEA. The FBI must go to Congress.

III. CALEA IS ILL-SUITED TO THE INTERNET; THE INTERNET AND SERVICES OVER THE INTERNET SHOULD NOT BE REQUIRED TO LOOK LIKE THE PSTN AND POTS

There is nothing untappable about packet or Internet technologies, as we explain further in Section IV below. Packet services currently available for voice and data are tappable at one or more points in the networks, and service providers are quite willing to work with law enforcement to satisfy interception orders quickly and fully.

However, as the Commission has described in the *IP-Enabled Services NPRM*, the Internet is fundamentally different from the traditional telephone network. Government agencies should not expect that surveillance will be carried out on the Internet the same way it is carried out in the circuit-switched telephone network. The digital revolution has produced numerous new means of communication and it is not reasonable to require that all of them identify communications and route traffic the same way that the telephone network does.

Yet the FBI's petition is trying to force the diversity of services available over the Internet into a single format resembling the telephone network. *See, e.g.*, Petition at 35 (“industry is required to provide the same level of capability for packet-mode technology as it does for circuit-mode technology”). In a telling omission, the FBI in its Petition fails to offer the Commission a road-map for translating the concepts of CALEA to the decentralized, user-controlled architecture of the Internet. This is especially true of “call-identifying information,” which has been the key term in dispute in interpreting CALEA. Nowhere in its petition does the FBI explain what is call-identifying information for an “always on” broadband service. Nowhere does the FBI state whether a broadband access service provider should be required to extract,

decode and format call-identifying information from a stream of bits. Yet these would be fundamental points of contention if the Commission were to extend CALEA to broadband services. The failure of the FBI to define “call-identifying information” for the broadband services it seeks to cover is itself evidence of the inapplicability of CALEA to the Internet and broadband applications.

A. There Is No Need for the Commission to Act to Cover Packet Technology Used by Telecommunications Common Carriers for Other than Information Services – Packet Technologies Are Already Clearly Covered

The FBI acts as if there is doubt about the application of CALEA to packet services. But there is none. The FBI acts as if the technology neutrality of CALEA were being ignored. For covered entities, it is not being ignored. The issue of packet technologies was settled some time ago, in the industry’s very first version of J-STD 025, in the Commission’s Third Report and Order of 1999, and in the Court of Appeals decision, *United States Telecom Ass’n v. FCC*, 227 F.3d 450 (D.C. Cir. 2000).

In the past, the FBI defended the industry treatment of packet technologies. In comments on CALEA standards filed with the FCC in 1998, the FBI and the DOJ stated that, with respect to packet switching, “the interim standard is fully consistent with CALEA.” Comments Regarding Standards for Assistance Capability Requirements at 1, *In the Matter of Communications Assistance for Law Enforcement*, CC Docket No. 97-213 (FCC, filed May 20, 1998). In its brief to the Court of Appeals on the petition for review of the Third Report and Order, the Justice Department stated, “From the standpoint of federal electronic surveillance law, however, there is nothing problematic about the J-Standard’s current arrangement.” Brief for the United States at 16, *United States Telecom Ass’n v. FCC*, Nos. 99-1442, 99-1466, 99-1475, 99-1523 (D.C. Cir., filed Mar. 6, 2000). It was CDT that had argued that carriers using packet

technologies should be required to separate call-identifying information from content when complying with a pen register or trap and trace order. The FBI, the Commission, and the Court of Appeals rejected those arguments.

So there is no need for the Commission to act on the FBI's petition to ensure that CALEA is applied in a technology neutral way to telecommunications common carriers.

B. CALEA As Interpreted by the Commission Would Be a Nightmare for the Internet

The FBI is trying to launch a process for which CALEA is unsuited and which could end up having disastrous implications for the Internet. Having previously defended industry packet standards that delivered the entire packet stream to law enforcement, the FBI is now claiming that industry packet mode standards are deficient. Petition at 35. If a standard is deficient, the FBI should file a deficiency petition, as it is entitled to do under CALEA. *See* 47 U.S.C. § 1006(b). Instead, the FBI has sought a declaratory ruling by means of the current Petition. It appears that the FBI considers the industry packet standards deficient for not meeting a “punchlist” for call-identifying information that is based on the model of the PSTN. Apparently, the FBI hopes that it can get a blanket ruling from the Commission on broad coverage of CALEA and then threaten a deficiency proceeding based on the punchlist to force broadband access providers to extract and format call-identifying information from the packet stream to meet the FBI's convenience. The Commission should not put itself or broadband service providers in that box.

If it grants the FBI petition, the Commission will be handing over Internet design powers to the FBI. Given the way CALEA has worked so far, the key power to define industry obligations has been exercised by the FBI. The FBI has imposed detailed CALEA obligations on telecommunications providers by adopting “requirements” documents defining very precise

features to be built into communications equipment and architectures. The FBI then provides these “requirements” to industry standards bodies as the minimum for CALEA compliance, threatening to challenge as deficient any standard that does not meet all of the FBI’s “requirements.” (When the FBI challenged the industry J-Standard as deficient, the FCC ordered the industry standard rewritten to conform to the FBI’s requirements, confirming the impression that the FBI will get everything it wants in the end). This shifts the dynamic of CALEA implementation in ways that Congress almost certainly could not have intended when it gave industry the authority to develop safe harbor standards. It is particularly inappropriate to the diversity and innovative nature of the Internet.

C. The Issue for Broadband, As It Was in Round One of CALEA Implementation, Would Be the FBI’s Desire to Pour Multiple Meanings into the Term “Call-Identifying Information” and to Expect Service Providers to Isolate and Format Call-Identifying Information on the Internet the Same Way It Is Treated in POTS

In the PSTN world, despite all the controversy over CALEA, there was no dispute over the interception of content. No carrier ever said that it would not have the ability to intercept any communication of a criminal or terrorist. The entire dispute concerned “call-identifying information.” The FBI convinced the Commission to pour into that term multiple meanings, forcing carriers to extract and format information that law enforcement had never obtained under pen registers and trap and trace devices before CALEA.

It is not difficult for last mile broadband access providers to intercept the packet stream to and from a particular customer. But it is quite difficult for last mile providers of always on services to extract anything that resembles “call-identifying information.” We expect that, if the Commission were to grant the FBI’s Petition, the debate over CALEA’s application to broadband services would really come down to one issue and its corollary: what is “call-

identifying information” (“CII”) in packet networks or “always on” services, and who bears the responsibility (and the cost) of pulling packets apart to isolate CII? The FBI apparently wants to define CII for packet services the same way that it is defined for traditional telephony. And it wants service providers to bear the responsibility of extracting the call-identifying information and formatting it for the government’s convenience.

The Commission should avoid the invitation to subject VoIP and other Internet services to the “punchlist” approach. This is precisely what Congress sought to avoid when it excluded the diversity of the Internet from CALEA.

IV. DENYING THE FBI PETITION DOES NOT LEAVE THE INTERNET IMMUNE FROM SURVEILLANCE.

Nothing sought in the FBI’s petition is required for law enforcement to be able to intercept the communications of criminals or terrorists who might use the Internet to communicate. Law enforcement can “wiretap the Internet” today, and has been able to do so since before the first implementation of the CALEA statute.

In crafting the CALEA statute – and in expressly exempting the Internet from its coverage – Congress made explicit its understanding that Internet communications were not immune from interception and surveillance: “information services can be wiretapped pursuant to court order, and their owners must cooperate when presented with a wiretap order.” *House Report* at 18. Congress made it clear that, while it was not imposing design mandates on the Internet, the Internet was not left out-of-bounds for lawful interception:

While [CALEA] does not require reengineering of the Internet, nor does it impose prospectively functional requirements on the Internet, this does not mean that communications carried over the Internet are immune from interception or that the Internet offers a safe haven for illegal activity.

Id. at 23-24.

As described below, CDT believes that law enforcement will be able to intercept all VoIP communications, and that none of those communications will be beyond the reach of law enforcement. Critically, although the Petition protests that law enforcement is hampered by Internet and VoIP technology, nowhere does the FBI identify *specific* technical situations in which it is unable to intercept a VoIP communication. Although we believe that the Commission is without authority to implement what the Petition proposes, before the Commission even considers such an action it must require that the FBI state – in specific detail – exactly what technical scenario is in fact beyond the reach of law enforcement. As detailed below, CDT believes that there are no such scenarios.

A. VoIP Technology (and Internet Communications More Generally) Can be Tapped and Intercepted

Without CALEA requirements being imposed, law enforcement will be able to tap VoIP communications (and can do so today). There are four basic VoIP scenarios confronting law enforcement, and all four can be tapped or intercepted. Although VoIP might not be tapped in the same way that the PSTN is tapped and might not produce the same information in the same format as the taps of the PSTN, the differences are not so debilitating to law enforcement as to require redesign of technology. Indeed, in some contexts interception of VoIP and other Internet communications is likely to provide law enforcement with *more*, not less, information about the communication.

To be clear, in some contexts and scenarios, law enforcement will have to learn and understand the internal protocols and formats used in VoIP communications. For example, many VoIP services use the Session Initiation Protocol, or SIP, for call initiating and setup functions. To the extent that law enforcement needs access to such information, it will need to understand such publicly available protocols.

An essential point, however, is that law enforcement *must* develop the capability to understand such protocols *regardless* of whether CALEA is extended to reach the Internet and VoIP communications. There will be a range of scenarios (generally encompassed in subsection 4 below) in which law enforcement will only receive (as it does today) the full Internet Protocol (IP) data stream for the target of a wiretap order. In those cases, law enforcement will need to be able to extract from that data stream SIP packets and other call setup information.⁸

The following four VoIP scenarios represent a distillation of a larger chart of specific scenarios that encompass all of the common methods of Internet access and VoIP usage. The chart is appended hereto as Attachment A. In the Petition, the FBI has not identified any particular scenario in which they are unable to obtain both content and call set-up information from service providers. In discussing these scenarios, we do not suggest that they are covered by CALEA – they are not. We present them here in order to make two points: (1) broadband services are already tappable, and (2) if Congress chooses to apply CALEA-like obligations on broadband access providers it will have to mandate obligations that are less rigid than CALEA as applied to the PSTN. In particular, Congress would have to take a different approach to call-identifying information.

⁸ As discussed in Section III.C above, it would be extremely difficult for an ISP that is only providing broadband access (and not providing VoIP services) to scan the IP data stream of a surveillance target and attempt to extract any third party VoIP communications services that the target is utilizing. It makes no sense to require ISPs to undertake an analysis of an IP stream that law enforcement can likely analyze far more easily than can the ISP (drawing on, for example, independent information gathered by law enforcement about what services a target might be using). Not only would such an approach force the ISPs to develop and deploy surveillance technology that the ISPs have no other legitimate use for (and, once developed, could be abused), but the approach would also likely harm investigations because hundreds or thousands of ISPs are less likely than the FBI to be able remain current on the latest communications technologies. The Commission must be crystal clear that this type of obligation should not be imposed on ISPs that provide only access services.

1. VoIP Services Provided by the Access Provider

In cases where VoIP services are provided by the same entity that is providing the target's access services (such as "voice over cable" offerings by the cable industry), law enforcement will be able to obtain both call content and call setup information from the single access/VoIP provider, although as noted above call-identifying information may not have the same components in the VoIP context that it has in the POTS context.

2. VoIP Services Provided by a Third Party Service Provider (with Call Content Passing Through the Third Party Network)

In cases where a separate company provides VoIP services, there are two basic scenarios that are possible, depending on the architectural model of the VoIP provider.

In the first of the two third-party provider scenarios, the call content passes through the network of the VoIP provider. VoIP providers that offer IP-to-PSTN services will likely see the call content flowing through network elements controlled by the providers. This scenario may also occur for some IP-to-IP connections, where the VoIP provider wants to maximize control over call quality.

In this scenario, law enforcement will have a choice. It could obtain call content and call setup information from the access provider of the target (with the access provider providing the target's entire IP data stream), or it could obtain the same information from the single VoIP provider (with the VoIP provider likely being able to provide more particularized call setup information, albeit not with the same exact components as law enforcement is used to in the POTS context).

3. VoIP Services Provided by a Third Party Service Provider (with Call Content Flowing Directly Between Calling Parties)

The second general scenario involving a third party VoIP provider is where the third party only provides call setup services, and the call content travels directly between the parties to the conversation. In this scenario law enforcement again has a choice. First, it could obtain call content and call setup information by way of a wiretap order to the access provider of the target (with the access provider providing the target's entire IP data stream). Second, it could obtain call setup information from the VoIP provider, and obtain call content by way of a wiretap order to the access provider (which again would be able to provide the target's IP data stream to law enforcement).

4. Self-Provided VoIP Services (with no VoIP Service Provider)

Finally, there will be cases where no company provides any VoIP services. This can occur in at least two situations: one or both of the call parties could operate their own SIP proxy servers (allowing call setup to be handled privately), or the parties could initiate communications directly on an IP address-to-IP address basis (which technically would occur without any "call setup" process, or possibly with a wholly out-of-band process).

In this scenario law enforcement will be able to obtain both call content and call setup information (to the extent it exists) from the access provider over which the call is placed (or, of course, the access provider of the recipient of the call).

B. Internet Communications (including New Technologies) Can be Intercepted at the Access Provider, But Law Enforcement Must Move into the Twenty-First Century to Make Use of Such Interception

More generally, all Internet communications, including the newest and most experimental technologies and protocols, can be tapped and intercepted by law enforcement through a wiretap

order directed at the access provider, without any need for a prior review by, or design mandate from, law enforcement or regulators.

Although as discussed above law enforcement will be able to tap and intercept VoIP communications, law enforcement will be required to become more technology-savvy to be able to respond to the new technologies used in the Internet (as compared to the telephone network). Underlying the FBI's Petition is a strong desire to have the signals and communications of the Internet translated back into the formats and modes of delivery of the PSTN. This approach is both unrealistic and, if permitted to control, would harm the development of new technology.

The backwards-looking approach of law enforcement can be seen in law enforcement's approach to standards development work. For example, CDT understands that in interactions with some standards bodies, the FBI has indicated that it was not willing to receive the SIP, or Session Initiation Protocol, packets that are used in many VoIP implementations for call-setup. Instead, CDT understands that the FBI has insisted that an ISP or service provider translate these packets into PSTN-style signaling. This makes little sense because SIP setup information simply does not translate cleanly into PSTN signaling, and because law enforcement would miss the additional information that SIP packets can provide. Instead of looking backwards, law enforcement must learn to understand the protocols and communications methods of the twenty-first century.

The evolving solution to E911 in the VoIP context provides a useful analogy. At the "Solutions Summit" that the Commission held on E911 and VoIP on March 18, 2004, Chairman Powell asked a critical question: should VoIP be forced to fit into the 30+ year old PSTN model on which today's emergency calling is based, or is now the time for the emergency calling system to take the "quantum leap" to new technology of the Internet and IP communications in

general. The strong consensus at the Solutions Summit was that now was the time for the 911 system to make a quantum leap into the twenty-first century. In the lawful interception context, law enforcement must also make that same quantum leap.

V. LAW ENFORCEMENT’S APPROACH WOULD SEVERELY THREATEN INNOVATION IN THE UNITED STATES, AND WOULD CERTAINLY DRIVE INNOVATION OFF SHORE

The Joint Petition asks the FCC to create a system under which any new technology that might replace a range of existing communications technologies must be reviewed and approved by the FBI and FCC before deployment. Such a prior-review requirement would destroy the United States’ ability to innovate on the Internet, and would in effect overturn the critical decisions of the FCC over the years that facilitated the rise of the Internet as a mass communications medium.

A. Law Enforcement’s Approach Would Roll Back the Development of Communications in the United States to Before the *Carterfone* Decision, which Fostered Innovation and the Advent of the Internet

The Commission is of course well familiar with the important part that its *Computer Inquiry* and related proceedings had in freeing American industry to innovate in the communications and computer fields. Critical among these decisions to the development of the Internet was the *Carterfone* decision.⁹

In that decision, the Commission resolved a complaint brought by Thomas Carter, challenging an AT&T tariff that prohibited the use of any device on the telephone system that

⁹ *In the Matter of Use of the Carterfone Device in Message Toll Telephone Service*, 13 FCC 2d 420 (1968). The significance of *Carterfone* and the *Computer Inquiry* proceedings is explored in Jason Oxman, Federal Communications Commission, Office of Plans and Policy, “The FCC and the Unregulation of the Internet,” OPP Working Paper No. 31, July 1999, at http://www.fcc.gov/Bureaus/OPP/working_papers/oppwp31.pdf.

was not approved by, and in fact provided by, the telephone company. The FCC overturned that tariff, and declared that telephone company customers could attached their own devices to the telephone network, so long as the devices did no harm to the network. This and other related decisions directly led to innovative uses of the phone system, including the broad use of the modem. Without this ability to introduce new technology into the network – free from review and control by the telephone company – online services such as CompuServe and Prodigy would not have occurred when they did, and the development and broad popularization of the Internet also would not have occurred as it did.

The key point of *Carterfone* is that it eliminated an innovation bottleneck in the form of the phone company. The FBI's petition, however, seeks to re-introduce the exact type of bottleneck eliminated in *Carterfone* – with the FBI and FCC in the position previously occupied by AT&T.

The Commission has a long and respected history of allowing the Internet, and the technologies on which the Internet is built, to develop and grow without interference or constraint. By granting the FBI's petition, the Commission would be adopting a radical, 180-degree change of course.

B. The Short History of the Internet is Full of Examples of Innovation Coming from Individual or Startup Efforts, and Such Innovation Would be Squelched by a Prior Authorization and Review Process.

As the Commission has observed over the past ten years, we have all witnessed a truly amazing and unprecedented amount of innovation in the development of the Internet. And a great deal of that innovation has been led by individuals or small groups of innovators. Although large American businesses have played an important part in the development of Internet

technology, single or small innovators have been crucial. Among the innovations led by small innovators are:

- the World Wide Web was originally conceived and created by one scientist, Tim Berners-Lee;
- the innovation of web-based e-mail was popularized by startup companies like Hotmail.com (acquired in 1997 by Microsoft);
- the innovation in instant messaging involved small startup companies like Mirabilis, creator of ICQ (acquired by AOL in 1998);
- individual innovators like Jeff Pulver and his Free World Dialup have made critical contributions to the development of VoIP.

Pulver's Free World Dialup is a prime example of the method of innovation that would be completely eliminated by the FBI's prior review proposal. FWD was created and released to the Internet, without any need for any specific technical design mandates or review processes. Once available on the Internet, it has become one of the VoIP success stories. It is far from clear that FWD would have developed in the United States if it had been required to undergo a review by the FCC and the FBI, with specific design requirements being imposed on its technology, all before any single subscriber could validate whether it was a good idea in the first place.

Open source development efforts are another creative and effective means for new technology to be explored on the Internet, and such efforts would be largely foreclosed by the FBI's demands. Such efforts are almost by definition done on a shoe string, and often without the central control that would be necessary to have the resulting product conform to the FBI's design mandates.

The proposed review and mandate process would be a crushing blow to the extraordinary innovation that we have seen over the past twenty years.

C. Technology Innovation Would Be Driven Off Shore

Of course, if the FCC imposed the FBI's review and design mandate process, innovation is unlikely to stop – but much of it would simply move off shore. The United States certainly does not hold a monopoly on Internet technology talent, and new ideas and technologies would simply be developed outside the reach of the FBI. The technology would eventually arrive on U.S. shores, but only months or years after it had been fully tested and deployed by overseas companies.

This would transform the United States from a technology leader to a technology follower, and would give an enormous advantage to overseas companies seeking to compete for U.S. technology dollars. Although the U.S. has already seen the dominance of, for example, Japanese technology companies in the development of CD and similar technology, the U.S. has up until now always been a driving (although not exclusive) force in the development of the standards and protocols on which new Internet technologies are based. There is little doubt that the United States' role in Internet innovation would decrease in the wake of a FBI/FCC review and design mandate process.

VI. THE FBI IS SEEKING TO REWRITE CALEA

Virtually every section of the FBI's petition asks the Commission to rewrite some aspect of CALEA. Having urged the Commission to bring the Internet into the regulatory scheme of CALEA (even though it was explicitly excluded), the FBI then complains in the second half of its petition about how poorly CALEA has worked. The FBI complains about “substantial confusion,” Petition at 33, “largely unsuccessful” implementation, *id.* at 34, and “problems and delays in the CALEA implementation process,” *id.* at 58. The FBI concludes that the CALEA implementation process, not only with respect to packet-mode technologies but generally, “is not

working.” *Id.* at 38. If the FBI is correct, it should ask Congress to revisit CALEA. But it is certainly not up to the FBI and the Commission to rewrite the law.

A. The FBI’s Pre-Approval Proposal would Shift Both the Burden of Going Forward and the Burden of Proof

The FBI would turn CALEA’s existing enforcement mechanism on its head.

Astoundingly, the FBI asks that the Commission “require any carrier that believes that any of its current or planned equipment, facilities or services are *not* subject to CALEA to immediately file a petition for clarification with the Commission to determine its CALEA obligations.” Petition at 34 (emphasis added). Similarly, if a carrier is “unsure” whether a new service is subject to CALEA, it should also seek clarification from the Commission. *Id.* at 54.

To put it bluntly, this is nonsensical. The statute places no burden on any carrier to prove that its service is not subject to CALEA before going forward with a new technology – that would be a hyper-regulatory burden of the worst kind. Moreover, the plain terms of CALEA state exactly the opposite. Under Sections 108 and 201 of CALEA, it is up to the Attorney General to bring a civil action against a telecommunications carrier, a manufacturer or a provider of telecommunications support services to enforce CALEA, 18 U.S.C. § 2522, and a court can enforce CALEA against a carrier only if “alternative technologies or capabilities or the facilities of another carrier are not reasonably available to law enforcement for implementing the interception of communications or access to call-identifying information,” and “compliance with [CALEA] is reasonably achievable through the application of available technology,” 47 U.S.C. § 1007(a).

The FBI similarly flouts the clear language of the statute when it asks the Commission to “establish procedures for enforcement actions against entities that do not comply with their CALEA obligations.” Petition at iv, 58. This asks the Commission to usurp a role Congress

granted to the courts, under procedures and standards that are favorable to service providers, under Sections 108 and 201 of CALEA. The statute makes clear that it is up to the Attorney General to bring a civil action in the appropriate district court to seek an order directing compliance; there is no need or authority for separate Commission action.

B. CALEA Already Has Clear Rules on Cost Allocation, Based on a Series of Factors That the FBI's Petition Ignores

The FBI further asks the Commission to “confirm that carriers bear sole financial responsibility for CALEA implementation costs for post-January 1, 1995 communications equipment, facilities and services.” Petition at 63. This directly contradicts and violates section 109(b)(2) of CALEA, which plainly states that the Attorney General bears the cost of implementation of CALEA with respect to equipment, facilities and services deployed after January 1, 1995, if compliance is not reasonably achievable. 47 U.S.C. § 1008(b)(2). In asking for a predetermination that all carriers are solely responsible for implementation costs for equipment, facilities and services deployed after January 1, 1995, the FBI is essentially asking the Commission to repeal Section 109(b)(1), which sets out a long series of factors that the Commission must consider in determining whether or not a carrier is responsible for the costs of compliance. 47 U.S.C. § 1008(b)(1).

The FBI also asks the Commission to establish rules that “permit carriers to recover from their customers the costs of developing and implementing CALEA intercept solutions in post-January 1, 1995 equipment, facilities and services.” Petition at 63. Yet again, this ignores CALEA’s existing framework for compensation. Under Section 109, CALEA specifically requires the FCC, on a case-by-case basis, to consider whether compliance “would impose significant difficulty or expense on the carrier *or on the users of the carrier’s system.*” 47 U.S.C. § 1008(b)(1) (emphasis added). Also under Section 301 of CALEA, carriers may petition the

Commission for recovery of CALEA compliance costs from the federal government. 47 U.S.C. § 229(e). CALEA does not contemplate a blanket rule, but rather an individualized evaluation prompted by a carrier's petition.

CONCLUSION

We urge the Commission to deny those portions of the Petition that ask that the Commission (a) extend the reach of CALEA to broadband Internet access, or to VoIP or other information services, (b) create a review process for future technology, or (c) create new procedures and enforcement mechanisms different from those already in the statute. Instead, the Commission should acknowledge the importance of the issues raised by the Petition, but also express its views about the importance of allowing the Internet to continue to develop free of regulatory burdens and technological mandates. In the end, if there are in fact problems that need to be addressed in this area, the FBI must seek solutions in Congress, not before the FCC.

Respectfully Submitted,

/s/

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

Dated: April 12, 2004

ATTACHMENT A TO CDT COMMENTS IN RM-10865

VoIP SCENARIOS AND MOST LIKELY POINTS OF LAW ENFORCEMENT INTERCEPTION

SU = Call Set Up CO = Call Content VP = VoIP Provider AP = Access Provider		TARGET'S INTERNET ACCESS METHOD						
		Traditional PSTN		Broadband Access				WiFi
		Dial-Up	Dedicated/ T1	Cable	DSL	Satellite	Wireless/ Powerline/ Other	Internet Café or Hotspot
VoIP PROVIDER TYPE OR METHOD	VoIP Provided by Access Provider	SU: AP CO: AP	SU: AP CO: AP	SU: AP CO: AP	SU: AP CO: AP	SU: AP CO: AP	SU: AP CO: AP	SU: AP CO: AP
	3rd party VoIP with content passed through	SU: VP CO: VP	SU: VP CO: VP	SU: VP CO: VP	SU: VP CO: VP	SU: VP CO: VP	SU: VP CO: VP	SU: VP CO: VP
	3rd Party VoIP with call setup only	SU: VP CO: AP	SU: VP CO: AP	SU: VP CO: AP	SU: VP CO: AP	SU: VP CO: AP	SU: VP CO: AP	SU: VP CO: AP
	3rd Party SIP server provider	SU: VP CO: AP	SU: VP CO: AP	SU: VP CO: AP	SU: VP CO: AP	SU: VP CO: AP	SU: VP CO: AP	SU: VP CO: AP
	Self-provision of SIP server/call setup capability	SU: AP CO: AP	SU: AP CO: AP	SU: AP CO: AP	SU: AP CO: AP	SU: AP CO: AP	SU: AP CO: AP	SU: AP CO: AP
	IP Address to IP Address VoIP	SU: AP CO: AP	SU: AP CO: AP	SU: AP CO: AP	SU: AP CO: AP	SU: AP CO: AP	SU: AP CO: AP	SU: AP CO: AP