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	)	

JOINT REPLY COMMENTS OF INDUSTRY AND PUBLIC INTEREST

SUBMITTED ON BEHALF OF

8X8, INC., CENTER FOR DEMOCRACY & TECHNOLOGY, COMPTEL/ASCENT, COMPUTER AND COMMUNICATIONS INDUSTRY ASSOCIATION, DIALPAD COMMUNICATIONS, INC., ELECTRONIC FRONTIER FOUNDATION, FREE CONGRESS FOUNDATION, INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA, MITEL NETWORKS CORPORATION, NET2PHONE, INC., PRIVACILLA.ORG, THE RUTHERFORD INSTITUTE, and THE VOICE ON THE NET (VON) COALITION

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: December 21, 2004

TABLE OF CONTENTS

SUMMARY

In 100 pages of comments, the DOJ/FBI fail to identify any rational basis meriting extension of CALEA to the Internet. Nor do they identify a single significant problem that would be solved by doing so. The DOJ/FBI comments, like their 72-page petition and the 50 pages of DOJ/FBI comments filed in response to the noticing of the petition, fail to identify what the problem is that the NPRM is attempting to solve. In the absence of evidence of any problem, it is impossible for the Commission to act. The record in this proceeding ties the Commission's hands, providing no basis upon which the Commission can rationally identify a problem or decide how it should be fixed or who should be responsible for fixing it.

Beyond failing to identify the problem, the DOJ/FBI comments include a series of extraordinary statements, the combined force of which is to show how inappropriate it is for the Commission to extend CALEA on the record before it. For example:

(1) The DOJ/FBI say that it is too "ambitious" to answer the fundamental threshold questions posed by the Commission, questions like "what do the basic requirements of CALEA mean in the packet context?"

(2) The DOJ/FBI decline to specify which service providers will be responsible for producing what types of information, seeking instead to exercise that authority in unreviewable closed-door negotiations with individual companies, most of which are under pressure to move products to market.

(3) While failing to provide the Commission and affected parties with the facts necessary to resolve some of the core issues at hand, DOJ/FBI at the same time argue that any limitation on their authority can be resolved only later, after a factual inquiry.

(4) The DOJ/FBI make it clear that, if CALEA is generically extended to VoIP (for which there is no statutory authority), they will conduct their own pre-approval process, whether the Commission authorizes it or not.

(5) DOJ/FBI propound a "blank slate" test of "reasonably available" that would effectively require innovators, as soon as an idea occurs to them, to consult with the FBI.

(6) The DOJ/FBI interpret the Commission's attempt at line-drawing – the line between managed VoIP and unmanaged VoIP – as no line at all, but rather as another ground for including information services within CALEA.

The record before the Commission – in light of the positions taken by the Department of Justice – cannot support the rules proposed in the NPRM. In these circumstances, the Commission has no choice but to step back and conduct a Notice of Inquiry proceeding, identify specific problems, and then craft solutions that respond to actual problems rather than vague assertions of need.

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	)	

JOINT REPLY COMMENTS OF INDUSTRY AND PUBLIC INTEREST

SUBMITTED ON BEHALF OF

8X8, INC., CENTER FOR DEMOCRACY & TECHNOLOGY, COMPTEL/ASCENT, COMPUTER AND COMMUNICATIONS INDUSTRY ASSOCIATION, DIALPAD COMMUNICATIONS, INC., ELECTRONIC FRONTIER FOUNDATION, FREE CONGRESS FOUNDATION, INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA, MITEL NETWORKS CORPORATION, NET2PHONE, INC., PRIVACILLA.ORG, THE RUTHERFORD INSTITUTE, and THE VOICE ON THE NET (VON) COALITION

8x8, Inc., Center for Democracy & Technology, CompTel/ASCENT, Computer and Communications Industry Association, Dialpad Communications, Inc., Electronic Frontier Foundation, Free Congress Foundation, Information Technology Association of America, Mitel Networks Corporation, Net2Phone, Inc., Privacilla.Org, The Rutherford Institute, and The Voice on the Net (VON) Coalition respectfully submit these reply comments on the Notice of Proposed Rulemaking and Declaratory Ruling ("NPRM"), as released August 9, 2004.

A broad group of industry and public interest groups submitted detailed initial comments raising a host of significant problems with the NPRM and its extension of CALEA to the Internet and to Internet applications.[1] Numerous other commenters raised similar or other major

[1] *See* Joint Comments of Industry and Public Interest, filed Nov. 8, 2004 (ET Docket No. 04-295) [hereafter "Industry & Public Interest Joint Comments"].

problems with the NPRM.[2] The number and breadth of the serious objections raised about the NPRM should give the Commission pause about continuing to a final rulemaking at this stage of the proceedings. The undersigned commenters submit the following additional concerns, primarily in response to the arguments advanced by the Department of Justice and the FBI in their November 8, 2004 comments.[3]

I. LAW ENFORCEMENT'S COMMENTS IN THIS RULEMAKING, LIKE THEIR JOINT PETITION, DO NOT PROVIDE THE FACTUAL FOUNDATION NECESSARY FOR THE NPRM'S PROPOSED REGULATORY SCHEME

As numerous commenters have repeatedly said, law enforcement has failed to present concrete evidence of a problem justifying extension of CALEA to the Internet. The DOJ/FBI comments and their predecessor filings have likewise failed to identify any solution that CALEA can be expected to yield that would address any actual problems faced by law enforcement. And

---

[2] Those commenters include:

AMA TechTel Communications, LLC
American Civil Liberties Union
BellSouth Corporation
Cingular Wireless LLC
Cellular Telecommunications and Internet Association
Earthlink, Inc.
EDUCAUSE Coalition
Electronic Frontier Foundation
Global Crossing North America, Inc.
GVNW Consulting, Inc.
Level 3 Communications, LLC
MaineStreet Communications, Inc.
Motorola, Inc.
Nextel Communications, Inc.
SBC Communications
T-Mobile USA, Inc.
TCA, Inc.
United States Internet Service Provider Association
Yahoo! Inc.

A handful of submitted comments supported the Commission's approach in the NPRM, and an additional group of comments did not squarely take a position on the extension of CALEA to the Internet.

[3] Comments of the United States Department of Justice (filed Nov. 8, 2004) [hereafter "DOJ Comments"].

finally, law enforcement fails to specify which entities would be responsible for solving which problems, while at the same time introducing tremendous uncertainty by stating that not every covered entity would face the same obligations.

On this record, the Commission cannot make a public interest determination concluding that CALEA must be extended to the Internet. In particular, the Commission cannot, as implored by the DOJ/FBI, make a coverage determination without making a capability determination. To do so would be to delegate to law enforcement agencies the same degree of control over technology that they sought in their initial digital telephony proposal over 10 years ago, which Congress rejected.

A. In More Than One Hundred Pages of Comments, DOJ/FBI Provide No Evidence that a Problem Exists that Extending CALEA Would Solve.

The Department of Justice has had four distinct opportunities to provide to the Commission evidence that law enforcement agencies have encountered *any* problem in intercepting Internet communications that justifies extension of CALEA. In their initial petition to the Commission, in two rounds of comments on the petition, and most recently in more than one hundred pages of initial comments on the NPRM, the Department of Justice and the FBI provide absolutely *no* evidence that they are unable to intercept Internet communications.

The Commission is obligated to undertake "reasoned decisionmaking" based on a sufficient factual record.[4] Without concrete factual input from law enforcement (input that is subject to review and comment by the public), the Commission lacks the foundation for rational decisionmaking and will be unable to justify any decision to extend CALEA to the Internet. This is not a situation where the Commission's inherent experience with telecommunications can

[4] *See Motor Vehicle Manufacturers Ass'n v. State Farm Mutual Auto. Ins. Co.,* 463 U.S. 29, 43 (1983).

provide the factual justification for the regulatory scheme created by the NPRM. Nor is this something that can be dealt with in *ex parte* submissions. Without factual input from law enforcement on the public record, so that the public and service providers can respond to it (and provide explanations for any problems cited), the Commission cannot extend CALEA to the Internet.

The Commission should not be persuaded by claims that CALEA problems cannot be publicly discussed. Congress managed to have a full dialogue about interception problems on the record when it adopted CALEA for the PSTN ten years ago. Second, if it were true that describing problems would provide tech savvy criminals with a roadmap for evading surveillance, the DOJ/FBI would already have done so in discussing the non-applicability of CALEA to e-mail or P2P voice services. There is no reason, on this record or elsewhere, to conclude that the debate concerning CALEA compliance cannot and should not be open and robust.

B. The Facts Presented by Law Enforcement Demonstrate that an Extension of CALEA Is Not Needed Because Law Enforcement Can Already Access Internet Communications.

The record is devoid of facts to establish that CALEA must be extended to the Internet. In fact the *only* significant facts presented by law enforcement establish precisely the opposite: that extending CALEA to the Internet is not needed to address any problems encountered by law enforcement. The facts presented by the New York Attorney General's office are so striking that they bear repeating. According to the November 8, 2004, affidavit of J. Christopher Prather:

> 16. The NY OAG has recently experienced the critical importance of the accessibility of VOIP technology to law enforcement's interceptions. Earlier this year, the NY OCTF executed a court-ordered wiretap on a Verizon wireline phone that was being used in furtherance of narcotics related crimes. Just a day or two after the interception was implemented, the target

> switched service providers, choosing a VOIP service provided by Time Warner Cable and retaining the same phone number. *Time Warner Cable cooperated* with the New York State police in facilitating the implementation of the court-ordered interception and *the wiretap was put into effect*. As a result of this wiretap, the OCTF wound up seizing four kilos of cocaine, an extraordinary amount for Central New York, and arrested eight individuals.[5]

Thus, the *only* factual evidence of actual lawful interception of *Internet* communications presented by law enforcement indicates that:

- the Internet Service Provider cooperated *even in the absence of an extension of CALEA*, and
- the wiretap was successful *even in the absence of an extension of CALEA*.

There is no evidence in the record now before the Commission to rebut these two critical facts.

Cable companies, like other broadband access providers and VoIP service providers, are already subject to surveillance assistance requirements, under 18 U.S.C. § 2510 *et seq.* ("Title III" or "Wiretap Act"),[6] 18 U.S.C. § 3121 et seq. (Electronic Communications Privacy Act "ECPA"),[7] and strengthened by the USA Patriot Act of 2001.[8] Congress adopted CALEA because law enforcement showed, and the telephone industry agreed, that technological changes were eliminating the features inherent in the PSTN that had made interception relatively easy. Congress adopted CALEA because, in the PSTN, the assistance requirements of Section 2518(4) were no longer sufficient – telecommunications carriers could no longer promptly satisfy law

[5] Prather Affidavit ¶ 16 (emphasis added), Comments of Eliot Spitzer, Attorney General of the State of New York (filed Nov. 8, 2004) [hereafter "New York AG Comments"].

[6] Title III was designed to protect the privacy of wire and oral communications while providing and specifying circumstances and conditions under which the interception of the content of wire and oral communications may be authorized.

[7] ECPA updated Title III and clarified privacy protections to account for new computer and telecommunications technologies and the collection of electronic call-identifying information (*e.g.*, pen registers on outgoing calls and trap and trace devices on incoming calls).

[8] USA Patriot Act expanded language to include "routing" and "addressing" information, and expanded the definition of "call processing" to include "the processing and transmitting of wire and electronic communications."

enforcement requirements on digital switches and wireless switches (the latter due to a capacity limit, not a capability problem) – and therefore CALEA's design mandate was needed for the PSTN. In contrast to the situation in 1994, the record shows that the intercept assistance mandate of 18 U.S.C. § 2518(4) is sufficient for broadband Internet and VoIP.

Based on this record, the Commission cannot conclude that there is a factually based need to extend CALEA to the Internet. In the absence of evidence of need, it is impossible to conclude that there is a public interest in extending CALEA. Moreover, to the extent the Prather affidavit suggests that savvy criminals will seek technologies not covered by CALEA, the NPRM does *nothing* to address that problem because the NPRM acknowledges (as it must) that there are significant voice and other technologies that are not covered by even a strained reading of CALEA statutory language.

The Commission should step back from this precipice, conduct a Notice of Inquiry proceeding, identify specific problems, and then craft solutions.[9] That approach, and in particular the development of a robust record on matters of critical concern, would be best for law enforcement and national security, as well as for privacy, innovation, competition, and consumers.

C. Vague Descriptions of Problems Submitted in Reply Comments Cannot Provide a Sufficient Basis for Commission Action.

If in their reply comments law enforcement submits evidence that some problems exist, there are still significant barriers that must be cleared before CALEA can be extended to the

[9] Although it is certainly possible that law enforcement has encountered a problem in packet networks, law enforcement has refused to put any such problems in the record. In the absence of a description of what those problems might be, it is impossible to tell whether they are a matter of training, or lack of technical sophistication on the part of government agents, or the result of discrete design problems that can be solved with more cost-effective solutions than a wholesale extension of CALEA to broadband providers and VoIP applications.

Internet (including, most fundamentally, the statute's express exclusion of Internet services from coverage, even if those services are a substantial replacement). However, if new evidence is submitted, and if the Commission suspects that such evidence could serve as the basis for rational extension of CALEA to the Internet, the Commission must permit an additional full round of comments on any such new evidence. To do otherwise would allow an end run around the rulemaking process. Without further proceedings, it would be impossible for the Commission to determine whether the asserted problems were real, and whether the best way to solve them would be by extension of CALEA to the Internet.

Critically, any assertion of a problem must be concrete, and cannot be vague, qualified assertions that law enforcement has encountered problems, such as the Department of Justice offered in September to the Energy & Commerce Committee of the U.S. House of Representatives:

> There have been occasions where, because of technological gaps with respect to certain services, telecommunications carriers were unable to provide, or were unable to provide in useable form, the content of communications or related information as required by court orders.[10]

Critically missing from this statement is any assertion that the problems relate to the *Internet*, or would be in any way be solved by the extension of CALEA to the Internet.

To the extent law enforcement attempts at this late date to come forward with facts demonstrating some need to extend CALEA to the Internet, the Commission must ensure that the factual assertions are sufficiently detailed to allow commenters to evaluate them. And critically, the facts must be relevant to the NPRM:

[10] Testimony of Laura Parsky, Hearing before the Subcommittee on Telecommunications and the Internet of the Committee on Energy and Commerce, U.S. House of Representatives, Sept. 8, 2004, at 7 [hereafter "Energy & Commerce Hearing"].

- the facts must relate to the Internet, and specifically to an Internet access provider and/or "managed" VoIP provider;

- they must demonstrate a failure to obtain information ordered by a court to be produced by an Internet provider;

- the facts should include what efforts, if any, law enforcement undertook to enforce the court order; and

- the facts must demonstrate that extending CALEA to *all* broadband Internet providers and *all* managed VoIP providers is necessary to address the problems identified.

Without concrete facts establishing a need to extend CALEA to the Internet, the Commission cannot fulfill its obligation to conduct only "reasoned decisionmaking."

II. LAW ENFORCEMENT'S FAILURE TO IDENTIFY THE CALL SETUP INFORMATION THAT WILL BE DEMANDED OF INTERNET APPLICATION OR SERVICE PROVIDERS MAKES CLEAR THAT THE COMMISSION LACKS CRITICAL INFORMATION NECESSARY TO EVALUATE WHETHER EXTENDING CALEA IS IN THE "PUBLIC INTEREST"

In its NPRM, the Commission specifically requested comment on one of the most critical questions pertaining to the extension of CALEA to the Internet and VoIP services: what does the term "call-identifying information" mean in the Internet context. NPRM ¶¶ 66-67. In their comments, however, the DOJ/FBI declined to respond to this absolutely vital, threshold question, stating only that they prefer to use the CALEA deficiency petition process to discuss the meaning of "call-identifying information."[11]

Moreover, it appears that as recently as September 8, 2004, the FBI had *not yet decided* what it intends to demand in the way of call-identifying information. When pressed by Congressman Cox on what would be involved with call-identifying information, Deputy Assistant Director of the FBI Marcus Thomas stated:

[11] DOJ Comments, at 42.

> 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.[12]

As the Commission is well aware, the first ten years of CALEA's application to the telephone system was marked by repeated disputes and litigation centered around a single primary topic: the meaning of call-identifying information. A great deal of the technological and financial burden imposed by CALEA's application to the telephone system were incurred because of the FBI's "punch list" demands on call-identifying information – demands that went beyond what was available with traditional analog PSTN wiretapping.

That controversy over the definition of call-identifying information in the PSTN was guided by Congressional testimony from the FBI Director[13] and by other legislative history describing what was meant by call-identifying information in the PSTN. Here, in contrast, the testimony of the FBI is that it does not yet know what constitutes call-identifying information for the Internet. Moreover, unlike the application of CALEA to the PSTN, where Congress made the public interest determination that CALEA should extend to the PSTN, here it is the

---

[12] Testimony of Marcus Thomas, Energy & Commerce Hearing, at 55.

[13] FBI Director Freeh testified:

> This information relates to dialing type information – information generated by a caller which identifies the origin, duration, and destination of a wire or electronic communication, the telephone number or similar communication address. . . . What I want with respect to pen registers is the dialing information: telephone numbers which are being called, which I have now under pen register authority.

Joint Hearings Before the Subcommittee on Technology and the Law of the Senate Judiciary Committee and the Subcommittee on Civil and Constitutional Rights of the House Judiciary Committee, Mar. 18 and Aug. 11, 1994 (S. Hrg. 103-1022), at 33, 50, available in part at http://www.eff.org/Privacy/Surveillance/CALEA/freeh_031894_hearing.testimony. In their report on the legislation, the House and Senate Judiciary Committees explained that, for voice communications, call-identifying information is "typically the electronic pulses, audio tones, or signalling messages that identify the numbers dialed or otherwise transmitted for the purpose of routing calls through the telecommunications carrier's network." House Report 103-827, "Telecommunications Carrier Assistance to the Government," Oct. 4, 1994, at 21, available at http://www.askcalea.net/docs/hr103827.pdf; id. at 16 (call-identifying information is "information identifying the originating and destination numbers of targeted communications").

Commission that must make a public interest determination before it decides to extend CALEA to the Internet (assuming the "substantial replacement" test can be used to sweep in information services, which it cannot).

If the Commission relies on the substantial replacement provision (and its required public interest test), the Commission cannot – as the Department of Justice prefers – wait until deficiency proceedings to consider the likely scope of required call identifying. Instead, the Commission must understand what burdens will be imposed by the NPRM *before* it finalizes the proposed rules. Yet the Commission lacks *any* information on what will almost certainly be the most problematic and costly of the FBI's demands on the Internet and VoIP communications – the FBI's requirements for call identifying information. Until DOJ and the FBI have decided what call-identifying obligations CALEA they will seek to impose on Internet and VoIP providers, it is impossible for the Commission to evaluate the burdens on Internet communications that will be caused by extending CALEA to the Internet. Without this information, the Commission cannot fulfill its obligation to determine whether imposing the burdens of CALEA on the Internet is in the "public interest."

In contrast, when it comes to an issue that may limit their discretion, law enforcement is quick to claim that a fact-finding inquiry is necessary. For example, the DOJ/FBI urge the Commission not to resolve CALEA standards issues without a "ripe set of facts." DOJ Comments, at 42. The question of what call-identifying information is reasonably available is "an issue of fact that can only be resolved in the context of a particular communication service." *Id.* at 44. Similarly, with respect to extension petitions, DOJ/FBI state:

> [W]hen evaluating section 109(b) petitions, the Commission should require that a carrier specify which of the specific section 103 capability requirements that carrier alleges it cannot satisfy, and the carrier should be required to produce evidence supporting its allegation for each requirement.

This insistence on specificity and fact-finding should not be limited. The position of the DOJ/FBI with regard to Section 109(b) petitions should also apply to the fundamental questions at issue in the NPRM. Thus, the Commission should require DOJ/FBI to specify which elements of call-identifying information a specific service cannot satisfy and should be required to produce evidence supporting its allegation for each punch list item.

The lack of basic information discussed in this section and in Section I – at this late stage of the proceeding and after three prior rounds of comments – should make clear that the Commission lacks the factual foundation on which to evaluate a proposal to extend CALEA. Although the NPRM requested a sweeping range of factual input, law enforcement has failed to come forward with the requested information (if in fact such information exists). In light of the broad failure of the rulemaking process to garner relevant facts, the Commission should put its NPRM on hold and should instead issue a Notice of Inquiry focused solely on building a factual record of any problems that need to be solved and the specific requirements the FBI seeks to impose on Internet providers.

The DOJ/FBI have compounded the problem by stating in their comments that call-identifying information will be interpreted differently for different covered entities. DOJ Comments, at 7. On the one hand, this is obvious, given the diversity of services that the NPRM would cover. But by raising the likelihood of differing interpretations of call-identifying information without resolving it, the DOJ/FBI is asking the Commission to delegate to them to decide, in private negotiations with innovators, what call-identifying information is for specific applications. This puts DOJ/FBI into the design process in a way that Congress never intended, as we explain further in the next section.

III. DOJ/FBI MAKES IT CLEAR THAT, IF THE COMMISSION RULES IN THEIR FAVOR ON THE QUESTION OF COVERAGE, THEY WILL EXERCISE DESIGN CONTROL AT THE PRODUCT OR SERVICE CONCEPT STAGE AND EXTEND CALEA BROADLY, REGARDLESS OF THE COMMISSION'S EFFORTS TO LIMIT THE SCOPE OF ITS RULING

In the NPRM, the Commission suggests a number of limitations on the reach of its rulemaking. Law enforcement, however, makes clear that they do not accept any of these limitations. In light of law enforcement's unbounded view of the reach of CALEA, and their stated intent to use the deficiency process to enforce their CALEA demands, the harmful impact of extending CALEA to the Internet will be far reaching.

The DOJ/FBI are obviously trying to maintain maximum flexibility, but in asking for a declaration of coverage with no declaration of obligation, the DOJ/FBI are essentially seeking a delegation of rulemaking authority that can only be exercised by the Commission. The DOJ/FBI want to decide, outside of the rulemaking process, what products or services are covered, what is call-identifying information, and who bears what obligation. In essence, they want the direct control that they sought with their first digital telephony proposal over a decade ago, which Congress refused to grant them.[14]

A. In Their Comments, Law Enforcement Makes Clear Their View that the Reach of CALEA is Far Broader Than That Suggested in the NPRM.

In numerous places, either expressly or implicitly, law enforcement rejects the Commission's efforts to narrow the harmful impact of extending CALEA to the Internet.

For example, the New York Attorney General flatly rejects the NPRM's proposed distinction between "managed" and "non-managed" VoIP. *See* New York AG Comments, at 9-10. The U.S. Department of Justice ("DOJ") does not expressly reject the managed/non-

[14] *See* Industry & Public Interest Joint Comments, at 16-22.

managed distinction, but will only agree that CALEA should not be extended to cover "non-managed" services "at this time." DOJ Comments, at 34. Moreover, DOJ's definition of "managed" is so broad as to sweep in most VoIP services. *See id.* at 32-33 (involvement in any on-going flow of information among Internet users should be considered "management"). DOJ does make express its view that "management and mediation may be present even in a service that does not interconnect with the PSTN." *Id.* at 33. Similarly, DOJ broadly defines "switching" to include "*anything* that can be characterized as switching," including apparently "non-managed" VoIP providers. *Id.* at 9 & n.39.

DOJ rejects other distinctions and limitations in the NPRM, including for example the focus on facilities-based broadband access provider. DOJ argues that resellers of broadband service (including, presumably, retail level resellers) should also be deemed to be covered by CALEA. *See* DOJ Comments at 35-36. Under the DOJ approach, it would appear that even a lone independent coffee shop or "Internet café" must become CALEA compliant if it sells access to the Internet to its customers.[15] This clearly is far from the intent or the statutory language of CALEA.

B. CALEA as Understood by the Department of Justice Would Effectively Require Pre-Deployment Review and Approval of New Technology By DOJ and the Commission.

Although the NPRM nominally rejected DOJ's proposed "prior approval" requirement, DOJ's comments make clear its intent to enforce such a regime in any event. DOJ's intent could not be clearer – it will seek to penalize service providers that do not submit their applications to pre-deployment review. This will be especially powerful since the DOJ/FBI make it clear that

[15] Furthermore, the DOJ approach to the NPRM raises the possibility that CALEA could be applied to consumers who allow the public to use their wireless access points (even if they do not "resell" the service for profit). It would not be in the public interest to interpret the Substantial Replacement Clause to include wireless access points.

they will read as broadly inclusive the managed/non-managed test that the Commission has proposed in an effort to limit the scope of its ruling. In its comments, DOJ made the following points:

- The mere availability of service, in DOJ's view, is enough to require CALEA compliance, even if no customers have ever utilized the service. *See* DOJ Comments, at 14.
- According to DOJ, "CALEA's purpose [is] to ensure solutions are built in pre-deployment." *Id.* at 21.
- DOJ warns that "[s]ervice providers would be well advised to seek guidance early, preferably well before deployment of a service, if they believe that their service is not covered by CALEA." *Id.* at 36.
- Indeed, according to DOJ, even "planned" services must be made to be CALEA compliant. *See id.* at 37.
- In DOJ's view, any service provider must submit their proposed new application to FCC and FBI review "well before deployment of the service in question" and "DOJ would certainly consider a service provider's failure to request such guidance in any enforcement action." *Id.* at 38.
- Fundamentally, DOJ insists that CALEA compliance must be a guiding factor in new technology when it is "first designed." *Id.* at 45. According to DOJ, "any definition of 'reasonably available' should be based on the technical solutions a carrier and vendor can achieve when they first design the network, not on the unfortunate realities that prevail after a non-compliant network has already been constructed." *Id.*[16]

Although the NPRM asserts that it is not creating a system of prior approval for all new technology, DOJ's comments make clear that this would be the precise effect of the extension of CALEA to the Internet, regardless of what the Commission says. The Department of Justice has made clear that it will attempt to penalize any service provider that does not, in the first instance, design new technology to achieve CALEA compliance. And, given the nature of the CALEA

[16] In a similar vein, the DOJ/FBI state that, in addition to broadband access and managed or mediated VoIP, "[o]ther functions may ultimately be found to replace substantial portions of local telephone exchange service," suspending the sword of Damocles over the heads of innovators. DOJ Comments, at 15-16.

process that the Commission is imposing on the Internet, the Commission will not be able to control the demands and actions of the Department of Justice in the standards development process. Without better guidance concerning the standards to be met, it is difficult to imagine how innovative service providers will be able to work through this process and bring new products to market in a timely fashion. Thus, if the Commission permits a system of prior approval – whether *de jure* or *de facto* – the harmful impact of the NPRM on technology innovation will be far reaching.

IV. THE UNBOUNDED, DISCRETION-BASED VIEW OF DOJ/FBI AS TO HOW THEY WILL APPLY CALEA WILL HEIGHTEN THE HARM TO INNOVATION AND THE INCENTIVE OF INNOVATORS TO MOVE OUTSIDE OF THE UNITED STATES

The NPRM if implemented will effectively create the system of prior review demanded by the FBI in its initial petition seeking to extend CALEA. Such a system – whether by regulatory fiat or practical reality – will have a devastating impact on the United States' ability to innovate on the Internet.

By empowering the FBI to bring deficiency proceedings against any Internet service or application provider that the FBI deems to be covered by CALEA, the NPRM will in effect undo some of the critical decisions of the Commission over the years that have facilitated the rise of the Internet as a mass communications medium. For example, in the crucial *Carterfone* decision,[17] the Commission took action to eliminate the bottleneck power that the incumbent telephone company had over the introduction of new technology into the phone network. This and other related decisions directly led to innovative uses of the phone system, including the

[17] *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.

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. The NPRM, however, effectively re-creates the type of bottleneck that hindered innovation in the PSTN, with the FBI and FCC in the position previously occupied by the phone company.

The extension of CALEA to the Internet and to Internet applications harms innovation, and the U.S. industry's ability to compete in the global market, in a number of ways:

- **CALEA will be a costly barrier to innovation.** The harm to innovation that will flow from the NPRM will come, first and foremost, in the form of erecting a major and expensive hurdle that all new U.S.-created communications technologies on the Internet will have to cross. Any innovator who wants to avoid being the target of an FBI deficiency petition will – prior to any implementation of a new idea – need to retain lawyers and lobbyists to spend months (or longer) working through the FBI/FCC technology review process. Many innovators simply will not be able to afford to bring new ideas to market (at least, not in the United States).

- **Small and individual innovators will be particularly hindered by a CALEA requirement.** A great deal of innovation in Internet technology over the past fifteen years 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 by Microsoft in 1997);

- the innovation in instant messaging involved small startup companies like Mirabilis, creator of ICQ (acquired by AOL in 1998);

- the widely used implementation of Secure Sockets Layer, Open SSL, that provides critical cryptographic protection to web browsing and Internet commerce, was produced by two individual Australians, Eric Young and Tim Hudson; and

- the SSH Secure Shell protocol, critical for many remote access services, was designed by an individual Finnish college student, Tatu Ylonen.

Innovation by individual or small innovators has been a hallmark of VoIP technology:

- individual innovators like Jeff Pulver and his Free World Dialup have made critical contributions to the development of VoIP;

- innovator Net2Phone is recognized as the first company to bridge the Internet with the public switched telephone network, and

- **S**kype, another emerging force in the VoIP world, was founded by individual technologists Niklas Zennström and Janus Friis.

Pulver.com's Free World Dialup ("FWD") is a prime example of the method of innovation that would be eliminated or driven overseas by the CALEA NPRM. 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.

- **Collaborative design efforts typical in Internet technology will be highly unlikely to exist under a CALEA mandate.** 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 specter of FBI deficiency proceedings. Such efforts are almost by

definition done on a shoestring, and often without the central control that would be necessary to have the resulting product conform to the FBI's design mandates. The extension of CALEA to the Internet would be a crushing blow to the extraordinary innovation that we have seen over the past twenty years.[18]

- **CALEA will inhibit or preclude technology and market development strategies that are very common on the Internet.** Two very common, and successful, approaches to developing technology and building a market used by Internet innovators (including major companies) are to (a) release "alpha" or "beta" versions of new products or technology to small groups of users (including volunteers previously unknown to the technology developers), and (b) to release free-of-charge initial versions of new products or technology. The NPRM's interpretation of the "substantial replacement" test (which rejects a market share analysis) would make such strategies far less viable, and the FBI's approach (where mere availability of a technology requires CALEA compliance) would in many cases make such strategies impossible. CALEA would effectively prohibit (in the U.S.) the highly successful Internet technology "sandbox" in which both innovators and early adopters can collaborate with low investment and risk.

- **CALEA will cause harmful delays-to-market.** It is unavoidable that a CALEA compliance mandate – especially the sweeping mandate envisioned by the FBI – will slow down

[18] There is also a risk that under the NPRM's overly broad understanding of "switching," it is possible that open source developers would be considered "providers of telecommunications support services." Many open source projects have at least some modicum of "addressing and intelligence functions for packet-based communications," and some may be used by telecommunications carriers. *See* NPRM ¶ 43 and Section 102(7) ("`telecommunications support services' means a . . . software . . . used by a telecommunications carrier for . . . switching functions"). For example, there are specific open source projects for routing software. See e.g. BIRD Internet Routing Daemon project (http://bird.network.cz/) and GNU Zebra routing software project (http://www.zebra.org/). Such an interpretation of CALEA would impose direct CALEA obligations on open source designers, the likely result of which would be to scuttle the technology development effort. This is yet another example of why CALEA – drafted to apply to the large telephone networks supplied by large equipment manufacturers – does not map well to the Internet.

the product development and thus marketing of U.S.-created technology. Such delays in bringing cutting edge products to market will hinder U.S. companies' competitiveness. The first to market has a significant competitive advantage, and U.S. Internet innovators will be less likely to have such an advantage.

- **CALEA will introduce significant additional uncertainty into the technology design process.** Far from promoting "regulatory certainty" as the Department of Justice suggests, *see* DOJ Comments at 17, the extension of CALEA to the Internet and Internet applications will significantly increase the *uncertainty* that will confront any company deciding whether to invest in new technology development. Today, in the absence of CALEA, a company's engineers can estimate how much design work will be required to complete a marketable version of a proposed new product. With a CALEA mandate – especially one in which the FBI refuses to disclose in advance its "call identifying information" demands – a company would be far less able to predict the magnitude of a particular design effort.

- **CALEA will force some new technologies to be far more complicated than otherwise necessary and thus may discourage design efforts.** According to the FBI, to be CALEA compliant a new technology must be *initially* designed to provide to law enforcement whatever bits of information the FBI specifies, *see* DOJ Comments at 45. Inherent in DOJ/FBI's position is the expectation that *additional* data would be generated and collected beyond what otherwise would otherwise be created within the technology itself. Such additional design requirements are certain to complicate any technology development undertaking.

All of the above factors lead to the inexorable conclusion that extending CALEA to the Internet and Internet applications will directly hinder and constrain technology development in the United States. The effort to design new Internet communications technologies will be more

complex, more costly, more time-consuming, and less predictable. CALEA was intended by Congress to be applied to the very mature and slow-to-evolve telephone industry dominated by a small number of major corporations. The Internet of today is a radically different technology development arena, and CALEA will have radically harmful effects on it.

Of course, if CALEA were extended to the Internet, innovation would be hindered, but is unlikely to stop entirely – some innovation 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. If the new technology does eventually arrive on U.S. shores, it would happen long after the new technology had been initially marketed and deployed by overseas companies. This would transform the United States from an Internet technology leader to an Internet technology follower, and would give an enormous advantage to overseas companies seeking to compete for U.S. technology dollars. Until now, the United States has been a leader in the development of the standards and protocols on which new Internet technologies are based, but such dominance would decline if the most innovative technology is ultimately developed elsewhere.

V. LAW ENFORCEMENT'S FAILURE TO DISCLOSE ITS CALEA REQUIREMENTS MAKES ANY SHORT COMPLIANCE DEADLINE GROSSLY UNFAIR.

The majority of the commenters (including, most notably, the DOJ/FBI) believe that the Commission's proposed compliance deadline of 90 days is unrealistic. The DOJ/FBI in fact proposed a deadline of one year. However, no deadline can be deemed realistic unless and until the Commission identifies and defines the standards with which companies must comply, including who is covered and what they are required to do.

As noted above in Section II, the Department of Justice has yet to disclose to the Commission what it will demand by way of call identifying information if the Commission allows the NPRM to go into effect. In fact, the FBI has not yet determined what it will demand.[19] Nevertheless, at the same time, DOJ asserts that carriers should be required to "immediately" comply with CALEA once the Commission extends CALEA to the Internet.

The Commission must not set a compliance deadline without knowing (at least in general terms) what actions will be required for compliance. The Commission cannot start any compliance clock ticking until after the FBI has disclosed its demands. And because the industry does not know what the FBI may ultimately require (in particular the call identifying information that the FBI will seek under CALEA), the undersigned cannot effectively comment on the appropriate amount of time needed to comply. Again, as suggested above, this rulemaking proceeding is simply not sufficiently developed for anyone – either commenters or the Commission – to make a rational decision about how much time is needed for compliance.

VI. SECTION 229 OF THE COMMUNICATIONS ACT DOES NOT EMPOWER THE COMMISSION TO IGNORE THE ENFORCEMENT MECHANISM SET UP BY CONGRESS IN CALEA.

Contrary to the Department of Justice's assertion, Congress did *not* create two "parallel" enforcement schemes with which the Commission can implement CALEA. *See* DOJ Comments, at 72. Instead, the CALEA statute created a single scheme – in Section 108 of the statute – to be used in cases where telecommunications carriers are alleged to not comply with the substantive mandates of the CALEA statute. In addition, Congress directed that the Commission integrate a few particular aspects of CALEA compliance (specifically some rules applicable to common carriers) into its larger responsibilities under the Communications Act. *See* 47 U.S.C. § 229.

[19] Testimony of Marcus Thomas, Energy & Commerce Hearing, at 55.

The Commission is not free to ignore the enforcement scheme created by Congress, and instead craft a new scheme of its own design. The Congressionally-designed enforcement scheme includes substantive protections that the Commission cannot replicate. In particular, Congress stated in Section 108 that no enforcement order could be issued unless a court found that "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." This imposes a high burden of proof on the government – it must rebut any showing that the interception can be carried out elsewhere. The DOJ/FBI did not include section 108(c) when they urged the Commission to adopt regulations by copying sections of the statute. DOJ Comments, at 75. They did so apparently on the ground that the section 108(c) determination was the kind that could be made only by a court. Yet surely, Congress would not have created two enforcement schemes, one with a very high burden of proof on the government and one without such a limitation. The enforcement schemes that the DOJ/FBI claims are parallel are not at all parallel if they could produce different outcomes. Yet that is what would happen under the DOJ/FBI proposal.

Furthermore, Section 229 is not parallel with Section 108 because Section 229 only applies to common carriers, while Section 108 applies to all telecommunications carriers, even those brought within the definition by the substantial replacement test.[20]

[20] Section 229(c) provides (with emphasis added): "The Commission shall conduct such investigations as may be necessary to insure compliance *by common carriers* with the requirements of the regulations prescribed under this section."

VII. THE DEFINITIONS OF CALEA CANNOT BE STRETCHED TO INCLUDE BROADBAND INTERNET ACCESS OR VOIP SERVICES

A. DOJ/FBI's Interpretation of "Switching" Is Incorrect, For It Would Sweep in Entities They Admit Are Not Covered by CALEA.

DOJ/FBI support their position with an elaborate analysis of CALEA's definition of "telecommunications carrier." Much of the DOJ/FBI analysis is irrelevant. For example, while it is true that that the Communications Act limits the definition of telecommunications to "transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or the content of the information as sent and received," the fact is that telecommunications does change the form of the information, from analogue to digital and back again and changes its content, such as by changing the speed dialed number into the full telephone number needed for call routing. In fact, many information services, such as email, do not change the form or content of the information and send it only to points specified by the user. Much of the DOJ/FBI analysis is also irrelevant in light of CALEA's express statement that information services provided by telecommunications carriers are not covered by CALEA (and VoIP remains an information service).

However, one aspect of the DOJ/FBI analysis deserves comment: their reliance on the term "switching" in CALEA's definition of "telecommunications carrier." The DOJ/FBI analysis proves too much: Under the DOJ/FBI interpretation of "switching" in CALEA, even narrowband ISPs, as well as Internet backbone operators, would be covered by CALEA,[21] which they clearly are not. Regardless of the contrast between CALEA and the Communications Act, it

[21] The NPRM indicated that switching includes the use of "routers, softswitches, and other equipment that may provide addressing and intelligence functions for packet-based communications to manage and direct the communications along to their intended destinations." ¶ 43. This would sweep in every part of the Internet, which is clearly wrong.

would violate all canons of statutory construction to give to the word "switching" in one statute (CALEA) a meaning that includes some Internet access providers and does not include others.

There is a simpler interpretation of the word "switching" in the CALEA definition: Congress was concerned in 1994 that the switching function performed by traditional telephone companies might be separated from the transmission function. The FBI and industry advised Congress that the CALEA solution would occur in the central office switches. With unbundling being debated as a regulatory mandate – the reforms of the 1996 Act were being developed at the same time that CALEA was being drafted – Congress did not want CALEA to be inapplicable to a situation in which an entity was responsible only for switching and had no transmission capacity of its own.

Faced with two interpretations of a term, the Commission is required to adopt the one that can be consistently applied. The DOJ/FBI interpretation of "switching" can be applied only to some Internet access providers, not to others. The definition of "switching" we propose – switching as performed in the PSTN – is consistently applicable.

B. The NPRM Ignores the Word "Replacement" in the "Substantial Replacement" Test

The Commission confuses "replacement" with "alternative." Consider the following: An electrical utility provides electricity to the public. It is classified as a public utility, and its rates and quality of service are regulated. It may be required to serve all of the community or provide special low rates to some customers, and it may even be required to share its lines with newcomers. An alternative energy company begins to offer solar panels to the public, and some members of the public start installing them and buy less power from the public utility. Some solar panel users are able to discontinue their purchase of electrical power altogether. They have chosen an alternative to the regulated common carrier, but we would not say that the solar energy

panels are replacing the electric power company, and we would not treat the solar panel provider as a public utility carrier and regulate its prices or impose on it social policy obligations imposed on such utilities.

Yet this is exactly what the Commission is proposing. Congress applied CALEA to common carriers and to those who were *replacing* common carriers, not to those who provide alternative communications technologies. The PSTN is not being replaced by VoIP. In fact, the PSTN is embracing VoIP to compete with the alternatives being offered by unregulated entities like cable companies. In the substantial replacement test, Congress intended to cover entities that were taking over the PSTN, even if they were only serving part of the public and therefore were not considered common carriers. Broadband access providers are creating an alternative path to the Internet and in some cases an alternative path to the PSTN, but they are not currently a replacement for the PSTN (and whether and when these providers will become a replacement is entirely unclear). Extending CALEA to alternative technologies and alternative networks is a judgment only Congress can make.

CONCLUSION

For the foregoing reasons, based on the current record, the Commission cannot proceed to finalize the rules advanced in the NPRM. The Commission should conduct a Notice of Inquiry proceeding, identify specific problems, and then craft solutions that respond to actual problems rather than vague assertions of need.

ON BEHALF OF

8X8, INC. (8x8.com)
CENTER FOR DEMOCRACY & TECHNOLOGY (www.cdt.org)
COMPTEL/ASCENT (www.comptelascent.org)
COMPUTER AND COMMUNICATIONS INDUSTRY ASSOCIATION (www.ccianet.org)
DIALPAD COMMUNICATIONS, INC. (www.dialpad.com)
ELECTRONIC FRONTIER FOUNDATION (www.eff.org)
FREE CONGRESS FOUNDATION (www.freecongress.org)
INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA (www.itaa.org)
MITEL NETWORKS CORPORATION (www.mitel.com)
NET2PHONE, INC. (www.net2phone.com)
PRIVACILLA.ORG (www.privacilla.org)
THE RUTHERFORD INSTITUTE (www.rutherford.org)
THE VOICE ON THE NET (VON) COALITION (www.von.org)

Respectfully submitted by,

/s/

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

Dated: December 21, 2004