Before the
Federal Communications Commission

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

Pursuant to the Commission's request for comments in its First Report and Order and Further Notice of Proposed Rulemaking[1] ("Order and Notice") concerning the Communications Assistance for Law Enforcement Act ("CALEA"), the Electronic Privacy Information Center ("EPIC") submits these comments.

EPIC is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC has participated in the debate surrounding CALEA and in the Commission's rulemakings on CALEA since 1994,[2] and maintains online resources on surveillance and other privacy issues at http://www.epic.org.[3]

The Commission specifically requested comments on whether CALEA requirements should be expanded to non-interconnected voice over IP ("VoIP") applications. EPIC opposes the expansion of CALEA requirements to VoIP communication. Altering or expanding CALEA's provisions is contrary to the plain

[1] *In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services*, ET Docket No. 04-295 (adopted Aug. 5, 2005; released Sept. 23, 2005).
[2] *See, e.g.*, *EPIC on Wiretap Bill Passage*, EPIC, *at* http://www.epic.org/privacy/wiretap/calea/epic_calea_statement.html
[3] EPIC maintains an online resource on wiretapping issues, *at* http://www.epic.org/privacy/wiretap/.

language and expressed legislative intent of the statute. As such, any expansion is a task that must be performed by Congress, and not by the Commission.

Furthermore, expanding CALEA into the developing ill-defined field of VoIP applications would subject potentially any Internet communication software to regulation. Requiring software developers to construct wiretapping provisions into their software interferes with privacy protection, makes applications vulnerable to attack, and increases the likelihood of crime. Expansion of backdoor surveillance requirements also increases the risk of privacy violations, including the unauthorized collection of third-party communications by law enforcement and private parties.

The Commission also has asked for comments regarding the possibility of creating separate sets of requirements for different types of service providers. EPIC believes that such rulemaking is beyond the authority of the Commission as specified in CALEA, and further believes that the Commission should not be extending the reach of CALEA beyond its intended scope.

I. Applying CALEA to Other VoIP Applications is Contrary to CALEA's Language and Intent

Extending CALEA requirements further would contradict the plain language of CALEA and ignore the legislative intent behind the statute. In passing CALEA, Congress explicitly excluded providers of Internet connectivity, messaging, and other communications software.[4] Extending CALEA even further to include non-

[4] "The definition of telecommunications carrier does not include persons or entities to the extent they are engaged in providing information services, such as electronic mail providers, on-line services providers, such as Compuserve, Prodigy, America-On-line or mead Data, or Internet service providers." H.R. Rep. No. 103-827, pt. 1 p. 18 (1994), *available at* http://www.epic.org/privacy/wiretap/calea/H_Rpt_103_827.txt. The

interconnected VoIP would thus require legislative revision of CALEA, which is beyond the Commission's statutory authority. The negotiations leading to the law's passage, Congress restricted CALEA compliance only to those telecommunications systems where law enforcement has traditionally had access.[5]

A. CALEA Applies Only to Telecommunications Services and Explicitly Excludes Information Services

Congress was clearly concerned about the implications of imposing CALEA requirements on information services such as the Internet and those commonly found on IP-based networks. The legislative history of CALEA unequivocally states that "[t]he 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."[6] The Committee Report also defines "telecommunications carrier" by reference to the Communications Act, thus excluding information services such as email and Internet access from its scope.[7] By

---

Committee also explicitly excluded messaging services that could transmit video or sound: "The term 'information services' includes messaging services offered through software such as groupware and enterprise or personal messaging software, that is, services based on products (*including but not limited to multimedia software*)…" *Id.*

[5] The Committee Report specifically stated:

> The Committee intends the assistance requirements…to be both a floor and a ceiling. The FBI Director testified that the legislation was intended to preserve the status quo, that it was intended to provide law enforcement with no more and no less access to information than it had in the past. The Committee urges against overbroad interpretation of the requirements…The Committee expects industry, law enforcement, and the FCC to narrowly interpret the requirements.

Id.

[6] H.R. Rep. No. 103-827, at 16.

[7] *Id.* at 17. As the Commission has noted in this proceeding, the Communications Act does not include integrated services "combining basic telecommunications transmission with capabilities for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information." Order and Notice at 9.

limiting the scope of its surveillance requirements to telecommunications carriers that use the public switched telephone network,[8] CALEA thus unambiguously excludes information services such as e-mail, groupware, messaging software and Internet access.[9]

Non-interconnected VoIP clearly falls outside the scope of telecommunications carriers originally contemplated by CALEA. It has no connection with the public switched telephone network, and it falls within CALEA's definition of information services, as multimedia messaging service software.

The Committee Report further supports the finding that non-interconnected VoIP is an information service, asserting that the "information services" exception is to be interpreted broadly to encompass developing technologies:

> It is the Committee's intention not to limit the definition of 'information services' to…current services, but rather to anticipate the rapid development of advanced software and to include such software services in the definition of 'information services.' By including such software-based electronic messaging services within the definition of information services, they are excluded from compliance with the requirements of [CALEA].[10]

Emerging software applications like non-interconnected VoIP were thus anticipated by Congress in drafting CALEA, and excluded from its provisions. Contrary to the Commission's assertions,[11] the "information services" exception was intended by

---

[8] The Commission's assertion that "public switched network" is distinct from "public switched telephone network" seems stretched, given that the same sentence identifies the components of that network as those entities "where law enforcement agencies have always served most of their surveillance orders." H.R. Rep. No. 103-827, at 16.

[9] CALEA § 103(b)(2)(A), *codified at* 47 U.S.C. § 1002(b)(2)(A). See also *United States Telecom Assoc., et al. v. Federal Communications Commission*, 227 F.3d 450, 455 (D.C. Cir. 2000) ("CALEA does not cover 'information services' such as e-mail and internet access.") (citing 47 U.S.C. §§ 1001(8)(C)(i), 1002(b)(2)(A)).

[10] H.R. Rep. No. 103-827, at 18.

[11] Order and Notice at 13.

Congress to be read broadly, and the services covered by CALEA were to be interpreted narrowly.[12]

B. VoIP is not a Replacement for Telephone Service for a Substantial Portion of the Public Within a State

The Commission rests most of its earlier expansion of CALEA provisions in the "substantial replacement provision" ("SRP") of § 102(8)(B)(ii). This provision provides that the Commission may find a switching or transmission service a "telecommunications carrier" if such service is "a replacement for a substantial portion of the local telephone exchange service" and if it is in the public interest to do so.[13] In addition to using a broad definition of "switching or transmission," the Commission found the "substantial portion" requirement met if "a service replaces any significant part of an individual subscriber's functionality previously provided via a circuit-switched local telephone exchange service."[14] This focus on the replacement of individual functions within an individual subscriber's services is contrary to the intent expressed in the language of the statute and in the Committee Report.

Nowhere in the text of the statute is the emphasis on an individual subscriber mentioned. The Committee Report also notes that a service falls under the SRP only if it "serves as a replacement for the local telephone service to a substantial portion of the public within a state."[15] This language clearly shows that Congress intended the Commission only to apply the SRP when it had deemed that a particular switching service had replaced the telephone network for a substantial number of people within a

[12] H.R. Rep. No. 103-827, at 15-16 (section entitled "narrow scope.").
[13] CALEA § 102(8)(B)(ii), *codified at* 47 U.S.C. § 1001(8)(B)(ii).
[14] Order and Notice at 6.
[15] H.R. Rep. No. 103-827 at 17.

given state. This interpretation is not only in line with the expressed intent in the Committee Report; it also reflects the policy goals of Congress in passing CALEA. CALEA's objectives were to provide appropriate tools to law enforcement by requiring assistance in surveillance of a telephone system that had evolved beyond simple wiretapping methods. CALEA was therefore intended to allow law enforcement to maintain their existing abilities as telecommunications technology improved and was adopted by the public. It was not, however, intended to require assistance from every new technology that any individual might use for interstate communication.[16] Before expanding the scope of CALEA applications, the Commission must first find that a service has replaced telephone service for a substantial number of people within a state. In this Order and Notice, the Commission has not provided any such evidence or made any such finding.

The multiplicity of services encompassed by the Commission's expansion of CALEA also belies the Commission's misinterpretation of the SRP. By defining "substantial replacement" as the replacement of a substantial function of a service available via a telecommunications service, the Commission has included within the scope of CALEA any service that may be provided over a telephone wire, whether that service is telephony or any of the various modes of communication available via the Internet. This would encompass not just the providers of the connections, but also the providers of devices or even any software program that makes use of Internet connectivity. The Commission's interpretation of the SRP would thus encompass something as simple as an instant messaging client, which after all replaces a function

[16] *See*, *e.g.*, text accompanying note 10, *supra*.

that could be performed via a modem over a telephone line. CALEA was clearly not intended to apply to all Internet-capable software and devices, as the Commission's interpretation of the SRP would have it be.

II. The Scope of Applications Covered by the Commission's Definition of "VoIP" is Unclear, and Overly Broad

The Commission has previously defined "VoIP services" as including "any packet-mode application" used for voice communications.[17] This encompasses a broad range of software applications, including many that are not traditionally associated with telecommunications carriers or even VoIP technology. The Commission recognized this in earlier proceedings, when it noted concerns that voice-enabled instant messaging or even voice chat between video gamers might be covered by CALEA.[18] Though the Commission then decided that such services were not contemplated by CALEA, it did so by noting that such services were "non-managed" services and that such services were "information services" statutorily exempted by CALEA. However, these distinctions appear to be moot in light of this current proceeding, in which the Commission rejected the distinction between managed and non-managed services[19] and also blurred the definition of "information services."

In the Order and Notice, the Commission uses the SRP to apply the statute to both broadband and interconnected VoIP. By reclassifying all facilities-based broadband providers as "telecommunications carriers" instead of "information services," the

---

[17] Notice of Proposed Rulemaking and Declaratory Ruling, *In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services*, 19 F.C.C. Rcd. 15676, 15693 (adopted, Aug. 4, 2004).
[18] *Id.* at 15707.
[19] Order and Notice at 20 ("we abandon the distinction…between "managed" and "non-managed" VoIP services").

Commission apparently applies CALEA to any method of Internet communication. Under the Commission's current interpretation of "telecommunications carrier" (i.e., any switching or transmission service that serves at least some function that the public switched network used to serve), a wide range of voice and data communications applications could be subject to CALEA. This could include instant messaging programs, chat room software, teleconferencing applications, and even in-game text and voice chat in online video games, none of which were previously provided by the public switched telephone network.

The Commission's broad application of the SRP makes such applications equivalent to telecommunications services. Under this rationale, and given the distributed nature of many developing communication methods, the SRP would include any Internet-capable software. The result would be that CALEA would require surveillance capabilities to be built into software applications that individuals place on their home computers. Such a requirement would mandate certain capabilities of any software that could be run on an individual's home computer, so long as the software could connect to the Internet. This would restrict consumers' ability to use their own computers, an interference with users' abilities to use Internet-capable computers for their intended purpose—to facilitate communication. EPIC warned the Commission against the application of CALEA to VoIP in 2003, urging for the creation of strong privacy protections in the nascent field.[20] EPIC continues to believe that a functional and trustworthy communications network can only be premised on privacy protection for

[20] Letter from EPIC to Michael Powell, Chairman, Federal Communications Commission (Dec. 15, 2003) *available at* http://www.epic.org/privacy/voip/fccltr12.15.03.html.

users of that network. Requiring backdoors in the security of a communications system undermines that trust.

Mandating backdoors on all communications applications would also interfere with the critical principles of "net freedoms" outlined by former Chairman Powell. Among the freedoms the Chairman listed was that users are entitled to run the applications of their choice.[21] Mandating that any applications allowing communication over the Internet meet the requirements of CALEA or other needs of law enforcement infringes upon this ability, which is crucial to promoting innovation, competition, and consumer protection.[22] Consumers should have the ability to control their own computers and the use of their own software without being subject to undue government regulation.

Furthermore, if the SRP is applied to such applications, CALEA could add cumbersome requirements to, and in effect determine the structure of, emerging modes of communication. This would be contrary to the purpose of CALEA, which was designed not to impede the development and deployment of new technologies, or to dictate design requirements.[23]

The field of Internet communication is still developing, as can be evidenced by the Commission's own attempts to categorize and re-categorize the various types of VoIP

---

[21] *See*, *e.g.*, Michael Powell, Chairman, FCC, Preserving Internet Freedom: Guiding Principles for the Industry, Remarks at the Silicon Flatirons Symposium on "The Digital Broadband Migration: Toward a Regulatory Regime for the Internet Age," University of Colorado School of Law, Boulder, Colorado (Feb. 8, 2004), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-243556A1.pdf, at 5.
[22] *Id.* at 6.
[23] H.R. Rep. 103-827 at 16.

and other communication methods even in this proceeding.[24] As new methods and modes of communication evolve within the flexible environment of Internet software development, any attempts to further subdivide the field into separate regulatory schemes not contemplated in the statute may soon become outdated. The result would be a cumbersome set of regulations that could chill competition and innovation, as novel services may find themselves regulated as an unintended consequence.

III. Expansion of CALEA into Other VoIP Applications Creates Privacy Vulnerabilities

In passing CALEA, Congress was careful to take privacy rights into account. Congress explicitly stated its intention to consider individuals' privacy interests in addition to the interests of law enforcement, existing industry, and developing industry.[25] Expanding CALEA to include non-interconnected VoIP services creates a host of practical difficulties in providing for individuals' privacy rights in the means and content of their communications.

A. Expanding CALEA to Other Services Increases the Risks of Privacy and Security Breaches

As has been stated, CALEA does not merely authorize surveillance—it dictates features that the developers of communications systems must accommodate in their designs. This means that surveillance backdoors must be affirmatively built into communications systems. Expanding CALEA beyond centrally-switched

[24] *See*, *e.g.*, Order and Notice at 20 (abandoning the distinction between "managed" and "non-managed" services).
[25] H.R. Rep. 103-827 at 12.

communications services will generate new security risks for users of a wide variety of systems.

EPIC recognized these dangers two years ago, when it wrote to the Commission that mandatory surveillance mechanisms in VoIP may also create security holes that unauthorized persons may exploit.[26] Security in a given communications system is not only dependent upon affirmative measures added after the system's construction; it also depends upon the structure and design of the system itself. Distributed systems, where a central provider may have no power to isolate individual communications, gain certain security attributes from that design. Requiring that such a system comply with CALEA could require centralization of its structure. This would not only obviate the advantages to efficiency and reliability that decentralized systems often boast, it would also remove an inherent security safeguard in the system.

Security experts have also noted this flaw in CALEA. Phil Zimmerman, a cryptographer and the creator of the PGP encryption program, notes that expansion of CALEA will increase vulnerability of access by "organized crime, foreign governments, and hackers," and that these and other bad actors can use information intercepted through these government-mandated backdoors to commit identity theft and other forms of fraud.[27]

B. Expanding CALEA to Packet-Switched Services Increases the Risk of Unauthorized Collection

---

[26] Letter from EPIC to Michael Powell, Chairman, Federal Communications Commission (Dec. 15, 2003) *available at* http://www.epic.org/privacy/voip/fccltr12.15.03.html.
[27] Larry Abramson, *Internet's Vulnerability to Wiretaps, 'Cyber Crime'*, (NPR radio broadcast Oct. 6, 2005), *available at* http://www.npr.org/templates/story/story.php?storyId=4947918.

Another difficulty is that applying CALEA to packet-based communications risks the unauthorized collection of third-party data. Any laws authorizing surveillance must protect against the collection of data from non-targeted individuals. Congress recognized this in the text of CALEA itself.[28] However, it has become apparent that law enforcement access to network traffic can result in the interception of communications of third parties not named or identified in court surveillance orders — a phenomenon that never occurred in the traditional, circuit-switched telephone environment. As such, the expansion of CALEA's technical requirements would make it difficult, if not impossible, for carriers to comply with the statutory command that they protect "the privacy and security of communications and call-identifying information not authorized to be intercepted."[29]

Internal FBI documents obtained by EPIC through Freedom of Information Act litigation show that surveillance conducted in packet-mode environments has resulted in the unauthorized capture of third-party communications. In a declaration submitted to the U.S. District Court for the Central District of California in January 2000, an FBI Special Agent described the operation of the Bureau's packet-mode surveillance device, Carnivore:

> *Although the program is capable of capturing more than the information authorized* under the [court] order, I or the installing technicians will configure the program in a manner that will prevent the program from capturing any information that is not authorized under the order.[30]

[28] CALEA § 103(a)(4), *codified at* 47 U.S.C. § 1002(a)(4).
[29] *Id.*
[30] Declaration executed by Edward Hill, dated January 31, 2000; available at http://www.epic.org/privacy/carnivore/fbi_dec.html (emphasis added).

The precautions described in the declaration apparently are not always effective. An internal FBI document shows that, little more than a month later, Carnivore surveillance performed by the Bureau's "UBL [Usama bin Laden] Unit" resulted in the unauthorized acquisition of "E-Mails on non-covered" individuals — a clear violation of federal wiretap law. The overcollection occurred after the Carnivore "software was turned on and did not work correctly." According to the Bureau document, the "FBI technical person was apparently so upset that he destroyed all the E-Mail take, including the take on [the authorized target]." The report, dated April 5, 2000, and sent to M.E. (Spike) Bowman, Associate General Counsel for National Security Affairs, describes the incident as part of a "pattern" indicating "an inability on the part of the FBI to manage" its electronic surveillance activities.[31]

Two Bureau memoranda written one week later further document Carnivore's tendency to acquire third-party data. The first, seeking "legal guidance," describes "the improper capture of data" as follows:

> On occasion we encounter non-standard implementation of transmission control and Internet protocols within a network or at an ISP. Encountering non-standard implementation has led to *inadvertently capturing and processing data outside the Order or Consent*. [32]

The response, apparently written by a Bureau attorney, notes that "[s]uch unauthorized interceptions not only can violate a citizen's privacy but also can seriously 'contaminate' ongoing investigations" and that such interceptions are "unlawful."[33]

---

[31] E-mail message to Spike Bowman, dated April 5, 2000; available at http://www.epic.org/privacy/carnivore/fisa.html.
[32] Memorandum, untitled and undated (but apparently April 11, 2000); available at http://www.epic.org/privacy/carnivore/questions.html (emphasis added).
[33] Memorandum "RE: Internet/E-Mail Intercepts," dated April 12, 2000; available at http://www.epic.org/privacy/carnivore/response.html.

In the face of these facts — and with no reason to conclude that the documented instances of unlawful overcollection of packet communications would not markedly increase if CALEA's requirements were extended to new packet-mode technologies — the Commission would abdicate its responsibility to "protect the privacy and security of communications not authorized to be intercepted"[34] were it to expand CALEA's reach further into IP communications.

IV. The Commission Lacks Authority under CALEA to Discriminate Between Types of "Telecommunications Carriers"

The Commission also has requested comments on what services should be exempted from application of CALEA, or whether different services should have different requirements for compliance. EPIC believes that such speculation is beyond Congress's grant of authority to the Commission in CALEA, since the statute contemplates only telecommunications carriers being covered. Congress has specifically granted the Commission, in consultation with the Attorney General, only the power to determine whether or not a telecommunications carrier should be exempted from the requirements of CALEA.[35] Nowhere in the statute does Congress suggest that the Commission should be able to determine different requirements for different types of carriers, simply because CALEA contemplates only two types of carriers: those that are subject to the requirements laid out by Congress, and those that are not.

CONCLUSION

In light of the legislative intent to limit CALEA's scope; the potential for interference with the freedoms of individuals with respect to their personal computer use;

[34] CALEA § 107(b), *codified at* 47 U.S.C. § 1006(b).
[35] CALEA, §102(8)(C)(ii).

the impediments presented in regulating a rapidly developing field of innovation, and the risk of unauthorized access to third-party communications, the Commission should resist the impulse to further extend the applicability of CALEA within the VoIP and broadband fields. EPIC urges the Commission to apply CALEA within its statutorily defined bounds of telecommunications carriers.

Respectfully Submitted,

/s

Marc Rotenberg
Executive Director

/s

Sherwin Siy
IPIOP Staff Counsel

Electronic Privacy Information Center
1718 Connecticut Street NW, Suite 200
Washington, DC 20009