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

In the Matter of:

Communications Assistance for Law Enforcement Act	**RM-10865**
Joint Petition for Expedited Rulemaking, filed by United States Department of Justice, Federal Bureau of Investigation and Drug Enforcement Administration	

To: Office of Engineering and Technology

COMMENTS OF ELECTRONIC FRONTIER FOUNDATION

Summary

The Electronic Frontier Foundation ("EFF") submits these comments in the above-referenced matter. EFF generally opposes the petition for expedited rulemaking brought by the U.S. Department of Justice, the Federal Bureau of Investigation, and the Drug Enforcement Administration (hereinafter referred to as "FBI").

The FBI petition is truly broad-ranging. It not only asks the Commission to rewrite the Communications Assistance for Law Enforcement Act (CALEA), but proposes a massive bureaucratic process under which the telecommunications industry would perpetually present new communications service offerings to the Commission (and presumably, the FBI) for CALEA compliance.

In EFF's view, the FBI petition presents three basic questions. First, is there any need to consider CALEA issues at this time? Second, does the FBI's petition propose reasonable steps for addressing CALEA issues? Finally, and most basically, does CALEA even make sense today? EFF contends that the answer to each of these questions is no.

EFF therefore recommends that the Commission either reject the FBI's petition in its entirety or exercise its authority under 47 U.S.C. § 229(a) to evaluate thoroughly the costs and benefits of CALEA implementation, including the very process of CALEA implementation, under the factors set forth in 47 U.S.C. § 1008(b).

I. Introduction and background

CALEA was enacted in 1994. The Commission has recognized that in enacting CALEA,

> Congress sought to balance three important policies: "(1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies." Based on these considerations, Congress envisioned that the requirements of CALEA would serve as "both a floor and a ceiling," defining the minimum capabilities that should be provided to law enforcement, while also establishing limits as to what can be provided.[1]

In this age of rapid technological innovation, however, ten years is a long time. CALEA showed its age in 1999, when the Commission invited an expert report from the Telecommunications Industry Association ("TIA") to address CALEA compliance problems associated with "packet-mode" communications under J-STD-025 ("JEM Report").[2] The JEM Report, submitted to the Commission in September 2000, made clear that packet-mode technologies raised serious legal, as well as technical, issues. For example, it found that the crucial statutory phrase "call-identifying information"[3] was "ambiguous with regard to packet communications," and that the TIA experts "could not define 'call-identifying information' for packet services."[4]

More fundamentally, the JEM Report noted that while the CALEA legal framework requires distinguishing "telecommunications services" from "information services," the two types of services may be "indistinguishable" "from a packet point of view."[5]

The problems of forcing CALEA requirements upon new technologies and a constantly changing communications system are even greater today. As far as EFF can determine, the legal and technical issues raised by packet-mode communications technologies remain largely unsolved outside of a few relatively well-defined areas.

EFF believes that the main reason for this and other CALEA compliance issues is simple: CALEA was neither intended nor written to apply to the Internet. Given the pace of

---

[1] *CALEA Further Notice of Proposed Rule Making*, 13 FCC Rcd 22632 (Nov. 6, 1998), at ¶ 3 (quoting H.R. Rep. No. 103-827, 103d Cong., 2d Sess., pt. 1, at 13, 22 (1994), reprinted in 1994 U.S.C.C.A.N. 3489 ("CALEA Legislative History")).

[2] *In the Matter of Communications Assistance for Law Enforcement Act*, Third Report and Order, 14 FCC Rcd 16794, ¶56 (1999).

[3] 47 U.S.C. § 1001(2) ("dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier").

[4] Joint Experts Meeting convened by Committee TR-45 of the Telecommunications Industry Association, *Report to the Federal Communications Commisssion on Surveillance of Packet-Mode Technologies* 10 (Sept. 29, 2000) ("JEM Report").

[5] Id. at 10 ("The point of communications setup may be the only time that a telecommunication service can be distinguished from an information service.").

technological innovation, attempting to apply CALEA to the Internet creates enormous legal, technical, economic and social problems.

This Commission has been committed to lowering government barriers to innovation and the deployment of innovative services. The FBI's proposed "solution" to its CALEA problems would raise those barriers by putting this Commission and the FBI in the role of technology gatekeeper. Even if the Commission and the FBI had the resources to attempt to play this role – which EFF seriously doubts – there is every reason to believe that the effort would be futile for law enforcement, dangerous to civil liberties, and prohibitively costly to innovation and the U.S. economy.

In short, adopting the FBI's proposal would contradict "the policy of the United States ... to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation."[6] EFF therefore urges that the Commission reject the FBI's proposal in its entirety.[7]

II. The FBI has presented no evidence that this rulemaking is necessary

The FBI's rulemaking petition would impose a massive bureaucratic structure upon innovation in communications. Yet the FBI has offered no evidence that this rulemaking is justified in terms of its civil-liberties and economic costs.

From the very beginning, the case for CALEA rested on weak evidence. The FBI in 1994 presented Congress with only 183 technology-based "problems" encountered by federal, state and local law enforcement agencies, probably a small percentage of the total number of electronic surveillance orders issued in that period.[8] Moreover, the public record merely indicates that law enforcement could not "fully" implement authorized electronic surveillance.[9] The FBI apparently did not assert that these problems materially affected the ability of law enforcement agencies to investigate crime.

The FBI petition presents no evidence that today's communications system materially affects law enforcement's ability to investigate crime. The FBI asserts that: "critical electronic surveillance *is being compromised today* by providers who have failed to implement CALEA-compliant intercept capabilities"; "[c]ommunications among surveillance targets are being lost"; "associated call-identifying information is not being provided" in a timely manner.[10] No evidence supports these assertions.

---

[6] 47 U.S.C. § 230(b).

[7] EFF also believes that the FBI's proposal, if accepted, would exacerbate the unsettled constitutional questions raised by CALEA, but we do not address those questions here. See CALEA Legislative History at 13 ("the question of whether companies have any obligation to design their systems such that they do not impede law enforcement interception has never been adjudicated.").

[8] CALEA Legislative History, at 15. It is not clear from the legislative history whether these problems were encountered in one year or over several years.

[9] Id. at 14.

[10] FBI Petition, at 8-9 (emphasis in original).

Similarly, no evidence supports the FBI's implicit claim that such problems materially affect criminal investigations. We do not know, for instance, whether law enforcement was able to gather evidence through other means. We do know that law enforcement authority to conduct electronic surveillance as well as to obtain records has increased dramatically since 1994.[11] Even before the enactment of the PATRIOT Act, the requirements for conducting "roving wiretaps" under Title III were significantly relaxed. The PATRIOT Act further relaxed restrictions on law enforcement authority for interceptions and pen register and trap-and-trace ("pen-trap") surveillance.

Equally important, the FBI is silent on how new technologies and information practices have enhanced or will enhance its ability to investigate crime. EFF challenges the FBI to demonstrate that it is worse off today under an honestly defined "status quo" – one not limited to areas that the FBI deems a "problem."

There are many reasons to believe that the FBI is, overall, better off today than before. The rise of the Internet has expanded both the amount and granularity of transactional and content information that can be cheaply captured by not only communications providers but also the businesses with which we transact.[12] Data aggregators like Choicepoint possess vast records of personal information that the FBI uses.[13] The debate over Total or Terrorism Information Awareness, as well as programs like MATRIX, shows that data-mining technologies are likely to assist law enforcement greatly. Simply put, more records are more cheaply available than ever before, making subpoenas and records searches a far more useful law enforcement technique.

Other technologies also cannot be ignored. The growth of public video-surveillance and face-recognition technology make more information available to law enforcement. The growing deployment of biometric, GPS (Global Positioning Satellite) and RFID (radio-frequency ID) technologies is making it easier to locate and track people.

The FBI has demonstrated considerable ability to adapt to new technologies on its own. The FBI's "Carnivore" technology allows it to gather packet-mode information more efficiently. Even end-user encryption – expressly permitted by CALEA – appears less problematic than the FBI had warned, given the FBI's technical creativity in using key loggers.[14]

In short, the FBI seeks to build a new bureaucratic structure for federal technology management on bald assertions that do not and cannot justify its sweeping proposal. At

---

[11] James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 Alb. L.J. Sci. & Tech. 65, 75-78, 82-84 (1997) (explaining how privacy protections have eroded while government surveillance power has grown).

[12] Id. at 82.

[13] Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S.Cal. L. Rev. 1083, 1095 (2002).

[14] See United States v. Scarfo, 180 F.Supp.2d 572, 581 (D.N.J. 2001).

the very least, the Commission should require the FBI to present meaningful evidence in support of its assertions. It is premature to embark on a costly and time-consuming rulemaking without such evidence.

III. The FBI's reading of CALEA is overbroad

Unsurprisingly, the FBI views CALEA as having only one purpose: "to *maintain* the ability of law enforcement to conduct lawful electronic surveillance despite changing telecommunications technologies."[15] Quite apart from the problem discussed above of what it means to "maintain the status quo," the FBI both overstates CALEA's statutory purpose and seeks to downplay CALEA's other two purposes, privacy protection and innovation.

A. Congress intended that CALEA be narrowly construed

A person who only read the FBI's characterization of CALEA would think that Congress created a broad mandate that all telecommunications be forever subject to federal design standards. Nothing could be further from the truth. When Congress stated that "[t]he break-up of the Bell system and the rapid proliferation of new telecommunications technologies and services have vastly complicated law enforcement's task," it immediately added: "The goal of the legislation, however, is not to reverse those industry trends."[16]

For example, Congress expressly noted that "from a privacy standpoint . . . the scope of the legislation has been greatly narrowed."[17] "Earlier digital telephony proposals covered all providers of electronic communications services, which meant every business and institution in the country. That broad approach was not practical. Nor was it justified to meet any law enforcement need."[18]

Similarly, Congress intended "that compliance with the requirements in the bill [] not impede the development and deployment of new technologies. The bill expressly provides that law enforcement may not dictate system design features and may not bar introduction of new features and technologies."[19] Furthermore, courts

---

[15] FBI Petition at 3 (emphasis in original).
[16] CALEA Legislative History, at 14.
[17] Id. at 18.
[18] Ibid. ("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. Further, such carriers are required to comply only with respect to services or facilities that provide a customer or subscriber with the ability to originate, terminate or direct communications.").
[19] Id. at 19.

> "may order compliance and may bar the introduction of technology . . . only if law enforcement has no other means reasonably available to conduct interception and if compliance with the standards is reasonably achievable through application of available technology. This means that if a service or technology cannot reasonably be brought into compliance with the interception requirements, then the service or technology can be deployed. This is the exact opposite of the original versions of the legislation, which would have barred introduction of services or features that could not be tapped."[20]

Finally, Congress clearly stated its intent that CALEA's assistance requirements "be both a floor and a ceiling" by "urg[ing] against overbroad interpretation of its requirements." Indeed, Congress "expect[ed] industry, law enforcement and the FCC to narrowly interpret the requirements."[21]

An example is CALEA's exclusion of private branch exchanges (PBXs). Congress recognized that "there will be times when the telecommunications carrier will be unable to isolate the communications of a specific individual whose communications are coming through a PBX," which "poses a minimization problem to which law enforcement agencies, courts, and carriers should be sensitive."[22] Indeed, Congress expressly stated that it did "not intend the exclusion of PBX's to be read as approval for trunk line intercepts. Given the minimization requirement of current law, courts should scrutinize very carefully requests to intercept truck lines and insist that agencies specify how they will comply with the minimization requirement."[23]

EFF therefore urges the Commission to reconsider its statement that "Congress intended the obligations of CALEA to have broad applicability, subject to the limitations explicitly contained" in the statute.[24]

B. Congress excluded many services, including "information services," from CALEA's requirements

Both the plain text and legislative history make it clear that Congress did not intend that CALEA be a broad mandate for "tappability." Even in 1994 Congress recognized that many communications services should not be subject to CALEA. As noted above, Congress expressly intended that services or technologies be deployed even if they could not be tapped, if reasonable.[25] Similarly, CALEA "does not limit the rights of

---

[20] Ibid.
[21] Id. at 23.
[22] Id. at 24.
[23] Ibid.
[24] In the Matter of Communications Assistance to Law Enforcement Act, Notice of Proposed Rulemaking, 13 FCC Rcd 3149, 3161 (1997).
[25] CALEA Legislative History, at 28-29 ("This subsection recognizes that, in certain circumstances, telecommunications carriers may deploy features or services even though they are not in compliance with the requirements of this bill.").

subscribers to use encryption."[26] Carriers only have a duty to decrypt or assist in decryption if they actually provide the encryption service and they possess the information necessary to decrypt the communication.[27]

Most important for present purposes, Congress clearly excluded "information services" from CALEA's requirements.[28] As the D.C. Circuit has said, "CALEA does not cover 'information services' such as e-mail and internet access."[29] The legislative history clearly states that "all information services, such as Internet service providers or services such as Prodigy and America-On-Line," are "excluded from coverage,"[30] and that "the bill does not require reengineering of the Internet . . . [or] impose prospectively functional requirements on the Internet."[31]

Furthermore, Congress intended that the term "information services" expand as technology advances. After expressly noting that "information services" includes all manner of application-based messaging services,[32] Congress stated its "intention not to limit the definition of 'information services' to such current services, but rather to anticipate the rapid development of advanced software."[33]

C. Broadband access is an "information service"

Accordingly, there can be no question that what the FBI sweepingly calls "broadband access service"[34] falls outside CALEA's definition of "telecommunications carriers" in

---

[26] Id. at 18.
[27] 47 U.S.C. § 1004(b)(3).
[28] 47 U.S.C. § 1001(8)(c)(i) ("telecommunications carrier" excludes "persons or entities insofar as they are engaged in providing information services"); id. at § 1002(b)(2) (assistance requirements "do not apply to" "information services"); CALEA Legislative History at 20 ("telecommunications carrier" definition "does not include persons or entities to the extent they are engaged in providing information services, such as electronic mail providers, on-line service providers, such as Compuserve, Prodigy, America Online or Mead Data, or Internet service providers.").
[29] U.S. Telecom Ass'n v. F.C.C., 227 F.3d 450, 455 (D.C. Cir. 2000).
[30] CALEA Legislative History at 18.
[31] Id. at 23.
[32] Id. at 21 ("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) of which Lotus Notes (and Lotus Network Notes), Microsoft Exchange Server, Novell Netware, CC: Mail, MCI Mail, Microsoft Mail, Microsoft Exchange Server, and AT&T Easylink (and their associated services) are both examples and precursors.").
[33] Ibid.
[34] FBI Petition, at 15 ("broadband access services" refers to "the process and service used to gain access or connect to the public Internet using a connection based on packet-mode technology that offers high bandwidth."); id. at 16 (broadband access services "includes the platforms currently used to achieve broadband connectivity (e.g., wireline, cable

47 U.S.C. § 1001(8). Clearly, a cable operator providing Internet access via high-speed cable modem service is not acting as a "carrier"; the Commission has found that cable operators acting in that role are information service providers.[35]

Indeed, the FBI implicitly recognizes in pressing its "replacement clause" interpretation, broadband access providers are not "common carriers for hire."[36] This is a wise concession. As the Commission has said, the entities subject to CALEA are "essentially, common carriers offering telecommunications services for sale to the public."[37]

Second, as noted above, Congress excluded "all information services, such as Internet service providers or services such as Prodigy and America-On-Line" from CALEA's coverage, and stated its intent that the Internet not be reengineered or be subject to prospectively functional requirements.[38]

Third, under CALEA, the term "information services" means "the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications,"[39] and expressly includes "electronic messaging services."[40] Given that both wireline and cable-modem broadband access services are "information services" under the Telecommunications Act,[41] all broadband access service generally is appropriately classified as an "information service."[42]

---

modem, wireless, fixed wireless, satellite, and power line) as well as any platforms that may in the future be used to achieve broadband connectivity").

[35] *Inquiry Concerning High-Speed Access to the Internet over Cable and Other Facilities*, Declaratory Ruling and Proposed Rulemaking, 17 FCC Rcd 4798 ¶ 7 (2002) ("Cable Modem Ruling"); but see Brand X Internet Services v. FCC, 345 F.3d 1120 (9th Cir. 2003).

[36] FBI Petition at 23-24.

[37] CALEA Second Report and Order, 15 FCC Rcd 7105 ¶ 10 (1999).

[38] CALEA Legislative History at 23.

[39] 47 U.S.C. § 1001(6)(A).

[40] 47 U.S.C. § 1001(6)(B)(iii). This definition is virtually identical to that used by the Telecommunications Act. 47 U.S.C. § 153(20) ("the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications and includes electronic publishing, but does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service.").

[41] In the Matter of Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, Notice of Proposed Rulemaking, (FCC 02-42) CC Docket No. 02-33, ¶ 16 (Feb. 15, 2002) ("Wireline Broadband Proceeding"); Cable Modem Ruling at ¶ 7.

[42] "Internet access providers do not offer a pure transmission path; they combine computer processing, information provision, and other computer-mediated offerings with data transport." Federal-State Joint Board on Universal Service, CC Docket No. 96-45, Report to Congress, 13 FCC Rcd. 11501, ¶ 73 (1998).

The FBI argues that Congress's statement that "the transmission of an E-mail message to an enhanced service provider that maintains the E-mail service" is covered by CALEA[43] should be understood to include Internet access generally. Given that in 1994, most people used their local exchange carrier to connect to their ISPs and thus the Internet, EFF believes that this statement simply reflects Congress's assumption that local exchange carriers would transmit e-mail from users to services like Compuserve.[44] A telephone modem can be tapped by making a sufficiently careful recording and then decoding the recorded signals; the ISP (e.g., Compuserve) would not need to be involved or even know that its subscriber was being tapped. Today, of course, many people do not use telephone modems to connect to the Internet, and e-mail is not necessarily stored or routed by one's ISP as it often was in 1994.[45] Congress did not anticipate that people would access the Internet in other ways; accordingly, Congress could not have intended that all of those other ways were automatically covered by CALEA.

D. "Broadband telephony" is an "information service" or an "application."

Similarly, "broadband telephony"[46] is an "information service" or, in some cases, simply an application. Pulver.com's Free World Dialup service is the most obvious example.[47] As one district court has found, Vonage is also an information service.[48]

While both these decisions are based on the Telecommunications Act, nothing in CALEA would alter their results. Both statutes define "information services" almost identically for present purposes. Indeed, CALEA includes one kind of "information service that is not included in the text of the Telecommunications Act: "electronic messaging services." Such services include "multimedia software," e.g., not only text messaging but also audio and video messaging.[49] Internet telephony services not only provide standard telephony features like call forwarding and call return but use the Internet to enhance these standard

---

[43] CALEA Legislative History at 23.

[44] CALEA focuses on "telecommunications common carriers, the components of the public switched network where law enforcement agencies have always served most of their surveillance orders." Id. at 18; id. at 24 ("The bill recognizes . . . 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.").

[45] The obvious example is Web-based e-mail. You can read Web-based e-mail from an Internet host that is not your home ISP. Even when you use your home ISP to read Web-based e-mail, it appears to your ISP that you are browsing at a particular Web site.

[46] The FBI defines "broadband telephony" as "the transmission or switching of voice communications using broadband facilities." FBI Petition, at 16.

[47] In the Matter of Petition for Declaratory Ruling that pulver.com's Free World Dialup is Neither Telecommunications Nor a Telecommunications Service, Memorandum Opinion and Order, FCC 04-27 (released Feb. 19, 2004).

[48] Vonage Holdings Corp. v. Minn. P.U.C., 290 F.Supp.2d 993, 1001 (D.Minn. 2003).

[49] CALEA Legislative History at 21.

features: one can listen to one's voice mail by visiting a Web page or via e-mail with sound attachments.

Finally, some entities that enable Internet telephony need not themselves use telecommunications; they simply offer applications outside the Commission's jurisdiction, not information services. Skype, for instance, is an end-user application for peer-to-peer voice communication just as Qualcomm's Eudora is an end-user application for e-mail communication.

E. Replacement clause analysis fails

The FBI argues that the Commission should find that broadband access service and broadband telephony providers are "a replacement for a substantial portion of the local telephone exchange service" and therefore included within the CALEA definition of "telecommunications carrier."[50] As noted above, however, Congress squarely excluded information services from CALEA's requirements and intended that the category of "information services" expand as technology advances.

Second, the FBI's sole argument here – that "broadband packet-mode networks may ultimately supplant narrowband circuit-mode networks altogether"[51] -- is disingenuous. In an attempt to paint broadband services as "substantial," FBI has lumped together many different services, like DSL, wireless, fixed wireless, satellite, power line and cable-modem service.[52] The replacement clause, however, applies to "a person or entity engaged in providing . . . service."[53] A DSL provider provides DSL service; a cable operator provides cable-modem service. It is inconsistent with the statutory text to treat these different services as one undifferentiated service. Moreover, Congress intended that such analysis examine effects on local exchange service "within a state."[54] Replacement clause analysis must proceed on a service-by-service, place-by-place basis.[55]

Similarly, the FBI does not say whether these individual services are being used in ways that are excluded from CALEA's requirements. Businesses, for instance, may use DSL for PBX service, which is not subject to CALEA. Such uses should not be counted in the replacement clause analysis.

---

[50] 47 U.S.C. § 1001(8)(b)(ii). This "replacement" test is also used in 47 U.S.C. § 332(c), which allows states to regulate wireless telephony rates if the test is met.
[51] FBI Petition, at 18.
[52] FBI Petition, at 16 (listing "platforms currently used to achieve broadband connectivity").
[53] 47 U.S.C. § 1001(8)(b)(ii).
[54] CALEA Legislative History at 21.
[55] Indeed, when convenient, the FBI argues that Commission rulings about a particular type of broadband service like cable-modem service should not be read to include other services. FBI Petition, at 25 n. 48.

Moreover, it is mere speculation to claim that any of these broadband services is a substantial replacement for local exchange service. The FBI says that broadband use is "surging,"[56] and that "cable-telephony lines constituted, in June 2003, about 11 percent of switched-access lines provided by competitive local-exchange carriers and about 2% of total switched access lines."[57] But it does not say that the percentage of local exchange service replaced by any service is "substantial."

Furthermore, "replacement clause" analysis requires a finding "that it is in the public interest to deem such a person or entity to be a telecommunications carrier for purposes of this title."[58] Aside from asserting a law enforcement or national security interest, the FBI simply does not provide any analysis of "the public interest." The FBI should at least address the impact of its unprecedented proposal on CALEA's other purposes: privacy protection and technological innovation.[59]

F. The FBI's proposal for identifying future CALEA-covered services and entities is inconsistent with CALEA

The FBI further argues that the Commission should establish rules for "the easy and rapid identification of future CALEA-covered services and entities."[60] In the FBI's view, these rules should presume CALEA coverage if: a service "directly competes against" an existing CALEA-covered service; an entity provides "wire or electronic communication transmission or switching service to the public for a fee"; or an existing CALEA-covered service migrates to a new technology.[61] This proposal would "benefit law enforcement, by ensuring that service offerings are CALEA-compliant on or before the date they are introduced to the marketplace."[62]

CALEA's text and structure do not support such a scheme of broad presumptions. As a threshold matter, CALEA coverage is limited to "telecommunications carriers"; other entities can be brought within CALEA only if the Commission finds, on a case-by-case basis, that they meet the two-pronged replacement clause test. The FBI essentially tries to reverse this built-in presumption by presuming the vast majority of future services to be covered by CALEA.

---

[56] FBI Petition, at 18 n. 40 ("both industry and trade press reports confirm that broadband use is surging").
[57] FBI Petition, at 19 n. 41 (citations omitted).
[58] 47 U.S.C. § 1001(8)(b)(ii).
[59] See CALEA Legislative History at 21 ("As part of its determination whether the public interest is served . . . the Commission shall consider whether such determination would promote competition, encourage the development of new technologies, and protect public safety and national security."); cf. 47 U.S.C. § 108(b)(1) (listing ten specific factors that the Commission should consider in determining whether CALEA compliance by a carrier is "reasonably achievable").
[60] FBI Petition, at 33.
[61] FBI Petition, at 33.
[62] FBI Petition, at 34; id. at 54 .

This approach is also inconsistent with CALEA's narrow, fact-intensive approach. As discussed above, replacement clause analysis must be performed on a per-service, location-specific basis and entails a fact-intensive inquiry into the public interest. Similarly, if the Commission is asked to determine whether CALEA's assistance requirements are "reasonably achievable" for equipment, facilities or services installed or deployed after 1995, it must consider at least ten different factors.[63] The Commission cannot substitute broad and vague presumptions for these fact-bound inquiries.[64]

More generally, the FBI asks the Commission to "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."[65]

CALEA does not support this sort of "opt-out" approach. Congress provided the FBI with mechanisms for enforcing CALEA obligations.[66] Under CALEA, a court decides these questions – and only at the behest of law enforcement. Congress presumably put the burden of raising these questions on law enforcement to ensure that only situations important enough to warrant action by the Attorney General would be adjudicated, thus sparing the Commission and industry the burden of addressing compliance issues that do not materially impact law enforcement.

Finally, ensuring CALEA compliance "on or before the date" that a service enters the marketplace is not a valid Commission goal under CALEA. Congress envisioned that "courts may order compliance and may bar the introduction of technology" only after finding that compliance would be reasonable, ensuring that carriers would have the protections of the judicial process and that services or technologies can be deployed if compliance would be unreasonable.[67] As Congress put it: "This is the exact opposite of the original versions of the legislation, which would have barred introduction of services or features that could not be tapped."[68] The FBI simply wants to rewrite the statute.

G. The FBI's proposal for packet-mode and future technology compliance is inconsistent with CALEA

More generally, the FBI seeks to turn the Commission – with the FBI's help -- into the nation's communications technology gatekeeper. The Commission would be forced to

---

[63] 47 U.S.C. § 1008(b).

[64] The broadest presumption is the "directly competes" presumption, which could sweep in any service that is used for communication. What does "directly competes" mean? Legions of antitrust lawyers will be happy to discuss this issue. What is a "service"? The FBI is likely to argue at some point that Internet application are "services."

[65] FBI Petition at 34; id. at 54.

[66] 18 U.S.C. § 2522.

[67] Ibid.

[68] Ibid.

decide what new technologies and services can be deployed. The FBI has offered little justification for this massive expansion of federal bureaucracy. It is bad enough that CALEA established technical design mandates for surveillance and that the FBI wishes to extend CALEA to the Internet; the FBI is also trying to add a huge bureaucratic apparatus for new service offerings.

1. Congress already provided the FBI with powerful tools to force carrier compliance

The FBI asserts that "the packet-mode standards that have been published are deficient" and that "there are alternative solutions for packet-mode technologies currently available."[69] If so, CALEA already contains mechanisms for requiring carrier compliance. When the FBI finds that a carrier cannot meet its CALEA obligations in assisting with a court order for electronic surveillance, it can seek a court order to compel the carrier to comply.[70] Even without a court order for electronic surveillance, the Attorney General may bring a civil action against any non-compliant carrier to force CALEA compliance.[71]

Moreover, nothing bars the FBI from petitioning the Commission for a ruling that CALEA's assistance requirements are "reasonably achievable" for any equipment, facilities or services installed or deployed after 1995.[72]

Congress anticipated that carriers might not comply with their CALEA obligations, and created a potent enforcement mechanism to address this issue. The FBI has not shown that it has been unable to use either of these procedures to enforce CALEA obligations, or that using these procedures is inadequate to meet its needs.

2. Packet-mode compliance presents significant legal, technical, and economic problems

The FBI's justification for proposing this new bureaucratic scheme is its apparent belief that packet-mode carriers are dragging their feet. EFF respectfully submits that there are more fundamental problems than carrier obstinacy.

First, carriers are likely unsure as to exactly what compliance means in the packet-mode context. The Commission itself admitted in 1999 that this was a hard problem, and the

---

[69] Ibid.
[70] 18 U.S.C. § 2522(a).
[71] 18 U.S.C. § 2522(b).
[72] 47 U.S.C. § 1008(b) provides that "a telecommunications carrier or any other interested person" may petition the Commission for such a ruling.

JEM Report found that packet-mode technologies do not fit well into CALEA's statutory scheme.[73]

The problem of packet-mode compliance is both legal and technological. For instance, CALEA requires that carriers be capable of providing "call-identifying information"[74] (CII) to law enforcement.[75] The proper meaning of CII is critical to determining what must be provided under pen register or trap-and-trace orders, which do not authorize the collection of communications contents, and thus to how carriers must design their networks. But as the JEM Report noted, there is no "call" in IP,[76] and the statute contains little guidance as to how the notion of a "call" should be applied in this context.[77] The TIA experts "could not define 'call-identifying information' for packet services."[78]

Much of the ambiguity surrounding CII arises from two basic aspects of Internet design: the so-called "end-to-end" principle; and encapsulation.[79] The end-to-end principle means that functions like reliability and security are generally allocated to hosts or computers at the edge of the network; for instance, retransmission due to packet loss is done by end systems instead of inside the network.[80] Encapsulation refers to the way that Internet traffic is defined by "stacked" protocol layers that allow different Internet hosts to focus only on the addressing information that they need to move packets.

One implication of the end-to-end principle is that "the IP transport network will not necessarily know what applications are being run over the network since there is no 'setup' in which the network participates. In fact, the network is designed not to know

---

[73] The FBI has modeled its plan after the Commission's E911 enforcement approach. It is apparent, however, that packet-mode CALEA compliance is a considerably more difficult issue, both legally and technically, than E911 compliance.

[74] CII is defined as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier." 47 U.S.C. § 1001(2).

[75] E.g., 47 U.S.C. § 1002(a)(2) (requiring carriers to "expeditiously" isolate and enable the government, "pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to a carrier" and "in a manner that allows it to be associated with the communication to which it pertains").

[76] JEM Report at 48.

[77] The FBI defines "call" to mean "a sequence of events beginning with an initial connection or facility request and ending with the final release of all facilities used." FBI, CALEA Implementation, *Electronic Surveillance Needs for Carrier-Grade Voice over Packet (CGVoP) Service* 2-2 (Jan. 29, 2003) [FBI CGVoP]. The FBI identifies 63 distinct law enforcement "requirements" and 22 distinct "objectives" for CGVoP surveillance.

[78] JEM Report at 10.

[79] EFF intends to expand its discussion of these and other issues in its reply comments.

[80] JEM Report at 46.

what application is being carried. The applications run end-to-end and the network just routes packets."[81]

Effectively, the end-to-end principle means that Internet services can be quite disaggregated and more innovative. Unlike the circuit-switched public telephone network, Internet communications need not flow through any bottleneck and need not be organized in any particular format. As a result, Internet users can use components created completely independently from any carrier. Many enhanced services are enabled on hosts reachable via the Internet, like DNS, e-mail servers, or Web servers: "The customer reaches these services just like it would any other service not offered by the service provider (i.e., via IP)."[82]

The combination of this openness to innovation and the relative ignorance of the IP network has at least one clear implication: carriers cannot keep up with the ability of innovators to create new applications, services, and protocols. When the FBI presented its Carnivore technology to the JEM II meeting as a means of separating CII from content, it admitted that "development of the filter protocol was intensive and fluid because of the ever changing nature of packet protocols and the constant introduction of new protocols; the Carnivore software or filters may need to be updated almost weekly to stay current."[83]

Similarly, the FBI's CALEA Implementation Section (CIS) suggested "examining the full packet stream . . . in order to gather the relevant call-identifying information" for delivery to law enforcement.[84] But CIS admitted that such examination "would place a high load on existing network elements in most architectures" and that "development of separation capabilities (i.e. filtering capabilities) within a service provider's network may be unrealistic as it would be highly resource intensive, very inefficient, and potentially inconsistent between providers."[85] Thus, "there was industry consensus . . . that it would not be feasible developing such a Separation Function independently or through a standards based process."[86]

For Internet telephony using a call management system (CMS),[87] the JEM Report found several surveillance problems. First, there is no standard CMS or call control protocol for IP. While most call control protocols for VoIP at that time exchanged IP address and

---

[81] JEM Report at 47.
[82] JEM Report at 47.
[83] JEM Report at 12.
[84] JEM Report at 12.
[85] JEM Report at 12.
[86] JEM Report at 12.
[87] "In general on an IP network, a call management system is a host attached to the IP network running call management protocols end-to-end over IP to its clients. For VoIP applications, the encoded voice stream is also carried over UDP/IP. In VoIP, the IP packets carrying voice are usually carried directly between the two endpoints involved in the call. The Call Management System is not involved in transporting the voice packets." JEM Report at 49.

port numbers with the CMS, this may not be true for future applications.[88] Second, because the CMS runs over IP, it can be located anywhere on a global IP network and could even be in a different country than the hosts to which it is providing service.[89] Third, the CMS can only know about its own "call events"; if you know the destination address of the person you wish to call, you can bypass the CMS entirely.[90]

More generally, the JEM Report noted a great difference between telephony and Internet call control protocols. While there are only a few base call control protocols with few variations for traditional telephony, there is no limit to the number or flexibility of Internet call protocols: "Therefore, nailing down a complete, fixed set of call events that are available via each protocol is close to impossible."[91] These problems are even greater for communications that do not use a CMS.[92]

EFF believes that these problems have intensified since the time of the JEM Report. It is in general harder for ISPs to tell what kinds of applications are being used. The practice of registering protocols and port numbers with the Internet Assigned Numbers Authority (IANA) has declined sharply; application developers today generally do not register protocols or port numbers in any central location and often choose ports at random or use ports that appear not to be in wide use.

Another development is the rise of tunneling, such as Virtual Private Networks (VPNs) that conceal both addressing and content information from the carrier. To the carrier, a VPN tunnel looks like a long stream of unintelligible, encrypted packets to and from the VPN host. It is our understanding that it is possible to use a VPN to access public Internet services in such a way that the carrier cannot tell what services, or even what kind of services, are being accessed.

Similarly, the proliferation of Network Address Translation (NAT) devices[93] and firewalls has led to increasingly sophisticated techniques for piercing or penetrating firewalls, often by disguising traffic or by allowing applications to use many different ports.

The use of NAT also makes it harder to associate users and IP addresses. NAT for packet-mode networks is roughly analogous to PBX for circuit-mode networks: both allow a group of users to be visible to the network only as a single user.[94] A NAT device

---

[88] JEM Report at 50.
[89] JEM Report at 50.
[90] JEM Report at 50.
[91] JEM Report at 51.
[92] JEM Report at 55-61.
[93] NAT devices are a kind of network gateway/router and could be a wireless access point, DSL or cable modem, modem/switch combination, general-purpose router, firewall or other device.
[94] A PBX system allows a group of users to share a single phone line (with its dedicated phone number) by using an adjunct processing scheme (phone number extensions). A

has at least two network interfaces. One interface is assigned a public, routable IP address by which the NAT device connects to the public Internet; a second interface is assigned a private, non-routable IP address via which the NAT device connects to a private network.

For present purposes, there are three key points about NAT: first, hosts on the public Internet can only address data packets to the NAT device's public IP address – they cannot directly detect the presence of the hosts or computers on the private network, because the NAT device rewrites the source address of packets originating from the private network; second, the sharing of a single IP address via a NAT device does not require permission from or even notice to any ISP or central entity; third, there is no theoretical limit to the size of the private network (or number of hosts) behind a NAT device.

The upshot is that all traffic coming from machines on the private network appears to come from a single node. Thus, if a surveillance target's computer is behind a NAT device, it becomes extremely difficult to identify the target's communications uniquely and thus to intercept only the target's communications (or to identify the target's "call-identifying information").

The use of NAT devices in connection with open wireless networks adds to the complexity, as EFF has observed in the context of the recording industry's efforts to identify alleged copyright infringers. When open wireless networks use NAT, the many parties who share the wireless access point may not have any formal relationship, may never have met, and may not even be aware of each other's existence.

Encapsulation raises even more difficult problems. The key issue here is the very meaning of CII – what is the distinction between "dialing or signaling information" and "communications contents" for Internet communications? The distinction was relatively clear for traditional telephony: telephone numbers are CII, and the conversations are contents. However, because Internet communications are encapsulated, each protocol layer is associated with different "signaling information."

Furthermore, what one layer considers to be "signaling information" is considered "content" for the next layer. To take a simple example, the FBI apparently takes the position that the message headers are CII, except for the subject header (which they deem contents). But consider the following sample SMTP session, where ">>> " prefixes client input, while the rest is server output:

```
220 owl.eff.org ESMTP Exim 4.22 Mon, 12 Apr 2004 11:48:18 -0700
>>> HELO ibook
250 owl.eff.org Hello adsl-68-120-144-116.dsl.snfc21.pacbell.net
[68.120.144.116]
>>> MAIL FROM: tien@eff.org
250 OK
```

NAT system transparently translates any number of private IP addresses to a single public address for both outgoing and incoming traffic.

```
>>> RCPT TO: chris@eff.org
250 Accepted
>>> DATA
354 Enter message, ending with "." on a line by itself
>>> Subject: testing
>>> To: Chris
>>> From: Lee
>>> Date: yesterday
>>>
>>> Hello, this is a test.
>>> .
250 OK id=1BD6U8-0008PZ-LX
>>> QUIT
```

From the SMTP perspective, HELO, DATA and QUIT are signaling information; MAIL FROM: . . . and RCPT TO: . . . are addressing information (envelope headers). But everything between DATA and QUIT is the "contents" of the SMTP transaction, which includes both the message headers and the body text. Thus, unless the concept of signaling information is specified for a specific protocol layer, one may be intercepting content rather than signaling information. The basic problem is that CALEA was not designed or intended to apply to the Internet, which functions very differently from the telephone network.

IV. The public interest would not be served by adopting the FBI's approach.

A. How much will it cost?

The FBI argues that carriers should be permitted to pass CALEA compliance costs to ratepayers, saying that "the costs of CALEA compliance for any particular ratepayer should be minimal."[95] The problem is that the FBI said nothing in its Petition about how much CALEA compliance will cost carriers and their subscribers. The Commission should be extremely wary of encouraging yet another federal "unfunded mandate."

If adopted, the FBI's proposal would also entail significant costs to the Commission itself. The general scheme for packet-mode compliance (which the FBI also wants to use for all future services that might be subject to CALEA) would entail:
--the Commission issues a public notice
--carriers must file a letter with the Commission about its compliance status, including its plans to offer services
--the Commission must respond to the carrier letters
--carriers must identify (6-mo) its chosen "technical intercept standard"
--the Commission must evaluate the carrier certifications
--carriers must certify (12-mo) that their suppliers or manufacturers have "deployed and made available the the intercept standard"
--manufacturers must also certify
--the Commission must evaluate the certifications.

[95] FBI Petition at 66.

Indeed, the FBI expects that "the Commission may need to establish separate phase-in schedules for separate packet-mode services,"[96] multiplying the costs of this process.

B. Expanding CALEA would be bad for security

As the JEM report correctly found, the additional complexity and additional points of attack that any surveillance system introduces into a communications system create new security risks.[97] Security engineers know that the number of devices (and programs) that process sensitive information should be minimized because each additional device (or program) processing sensitive data creates new risks of exposure or tampering. This observation echoes the maxim that a chain is as strong as its weakest link; adding additional links to a chain is likely to weaken it, and adding additional devices or functionality to a network is likely to create new opportunities for attack.

These opportunities can be exploited not only to invade individuals' privacy but also to practice financial fraud and industrial espionage, since financial transactions and sensitive business information are increasingly transmitted over public networks.

The security risks of deploying network surveillance technologies include, but are not limited to, the following.

Misconfiguration or misdeployment. Surveillance hardware and software may be difficult to configure correctly; inevitably, carrier staff may misunderstand surveillance features and deploy surveillance capabilities incorrectly, leading to unauthorized access, or enhancing any of the other risks described below.

Vulnerabilities in operating systems or commodity software within surveillance devices. Many surveillance devices run on a mainstream operating system such as Linux, Solaris, or Microsoft Windows; each of these operating systems has or bundles software that regularly experiences reports of remotely exploitable vulnerabilities, entirely outside the control of the developers of surveillance devices.

Vulnerabilities in surveillance software access control or reporting functions. Surveillance software itself may contain software defects such as buffer overflows that may lead to remote compromise of a surveillance device. This compromise could lead to changes in the function of the surveillance device, to surreptitious illegal surveillance, or to attacks on other systems.[98]

---

[96] Id. at 40.

[97] JEM Report at 47.

[98] Robert X. Cringely reported in July 2003 that existing CALEA deployments had actually been compromised in this way. See http://www.pbs.org/cringely/pulpit/pulpit20030710.html (accessed April 9, 2004). By personal communication, Mr. Cringely indicated to EFF that he had learned of these compromises from two independent and reliable sources whom he was not at liberty to identify.

Vulnerabilities in surveillance software recording, parsing, or minimization functions. Surveillance software that contains functions equivalent to a network protocol analyzer may contain software defects such as buffer overflows within the protocol analysis function that may lead to remote compromise of a surveillance device.[99]

Abuse of authorized access. Network surveillance technologies provide attractive opportunities for law enforcement, carrier personnel, and the developers of surveillance technologies to abuse their authorized access. The more that surveillance technologies provide an opportunity to target a particular individual's or organization's communications, the greater will be the incentive for individuals with authorized access to intercept communications to abuse that access. In some cases, audit trails may mitigate certain kinds of abuse, but they will not defend against abuses by developers of surveillance technologies, especially if purchasers of surveillance devices cannot easily verify whether the devices perform according to their published specifications.[100]

Network architecture decisions that reduce security. Designing for surveillance may encourage network developers to centralize their networks (forcing all data to pass a particular point or network segment) or to duplicate or record traffic, causing it to appear on interfaces, segments, or recording media where it would otherwise not have appeared. All these decisions can create new avenues and opportunities for attack.

---

[99] Packet dissector functions, which interpret network protocols, are normally written in non-bounds-checked programming languages for speed. A series of remotely exploitable buffer overflow bugs have recently been reported in packet dissectors used within various network analyzers. See http://www.ethereal.com/appnotes/ (accessed April 9,2004) (13 advisories about recent security-critical flaws in Ethereal network analyzer, including multiple remotely exploitable vulnerabilities in various protocol dissectors). The tcpdump network analyzer has had similar problems. In each case, code had been added to a network analyzer to help it interpret packets associated with a particular protocol. But in each case, because of logic errors or mistaken assumptions on the part of software developers, a slightly non-compliant variant of a protocol would confuse the protocol analyzer and make it behave incorrectly in a way that might be remotely exploitable. For example, just performing network surveillance using tcpdump or Ethereal would have allowed the people being monitored or perhaps any Internet user to remotely gain control of the monitoring device. Packet dissector buffer overflows are now widely recognized as their own family of network software vulnerabilities. As the FBI communicated to JEM, it will always be necessary to write and rapidly deploy more and more protocol-specific code as new protocols are invented. If current experience is any indication, each one of these protocol-specific capture programs may introduce new flaws. Automated minimization plainly requires protocol-specific code, so that any device that attempts to implement minimization could be at risk of overflows.

[100] When a surveillance device is connected to the Internet, it may be able to leak the concept of captured communications to a third party in a way that is relatively difficult to detect. Steganographic or "information-hiding" techniques may be employed to disguise the presence of an information leak.

Diminished competition harms security. The anticompetitive effects of technology mandates may tend to reduce the general quality of products provided in the markets for networking hardware and software. This loss of quality may include security problems or an inadequate response by vendors to security problems when problems are discovered.

Risks from creating packet logs. If packets are preserved in swap files (virtual memory) or even in random-access memory, an attacker may be able to recover their contents even after a significant amount of time has lapsed. This is true whether the attacker is a physical attacker (such as a carrier employee abusing authorized physical access to a surveillance device, or a physical intruder at a carrier's premises) or a networked attacker (using an attack such as a buffer overflow to take control of a device remotely). It is known to be relatively difficult to reliably and permanently erase sensitive data recorded within a device.[101] Deploying a surveillance device may result in recording the contents of sensitive packets which otherwise might not have been recorded at all, even packets whose contents were not authorized by law to be recorded and even packets sent by people who are not targets of surveillance at all.[102]

Additional code paths in network equipment. Not only does the additional software necessary to implement surveillance create risks of unauthorized access (since it is significantly harder to verify the correct function of the software system), it also may create opportunities for attacks on availability – so-called "denial of service attacks." A more complex software system has more software that may crash or be crashed. The packet dissector flaws described above may in some cases be exploitable in ways that cause devices to slow or stop functioning entirely, providing a route for an attacker to interfere with the smooth operation of network infrastructure.

Continuous source of new risks in software updates. Surveillance software, as the FBI explained to the JEM committee, must be continually modified in an attempt to keep up with developments in communications technology. Information about new protocols, and corresponding packet dissectors, logging features, etc., must be added. (As we have noted, surveillance capabilities will constantly lag behind because people are constantly developing new ways of communicating with one another.) As a result, surveillance

---

[101] See, e.g., Peter Gutmann, "Secure Deletion of Data from Magnetic and Solid-State Memory" (discussing possibility that data believed to be deleted can be recovered from physical media even after it has already been overwritten), available at http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html (accessed April 9, 2004). Most modern computer operating systems may use a computer hard drive for temporary storage space (virtual memory) and will transparently copy contents of RAM onto swap space on a hard drive. In many cases, this can result in cryptographic keys or other sensitive data (such as the content of captured packets) being undetectably written to disk and persisting there for some time. Avoiding this possibility may require special precautions which vary from operating system to operating system.

[102] Since a computer implementing a minimization function must process the contents of packets in order to carry out this function, the packets that are discarded by the minimization function must at least initially have been present in the computer's memory and therefore may be inadvertently recorded, as described earlier.

devices must include some means of being updated regularly. Where this update feature is present, it carries its own security risks – since an attacker may try to use it to perform an unauthorized update to surveillance software. And even successful software updates will make a surveillance-related code base grow larger and may carry with them new vulnerabilities.

Risks to confidentiality of intercepted information. When intercepted communications information is delivered to law enforcement over public networks, it risks exposure. The secure delivery of such information requires a cryptographic infrastructure, may require placing trust in the proper behavior of many carrier personnel, and can suffer major failures of confidentiality if relevant keys are disclosed. The successful illicit interception of surveillance information in the process of being delivered to law enforcement will lead to new invasions of a surveillance subject's privacy may also disclose the identity of law enforcement targets. The necessary technology to secure the on-line delivery to law enforcement of surveillance information, and the associated cryptographic key management, becomes increasingly complex as more law enforcement entities seek to receive intercepts on-line and more carriers are asked to provide them.

There is no reason to believe that surveillance devices in general will suffer a lower rate of vulnerabilities than other network software and devices. Indeed, since surveillance functions frequently incorporate or are implemented on top of commodity operating systems, they may inherit all of the security risks associated with other devices together with their own unique risks.

Successful attacks have been mounted against devices that perform network surveillance. While we cannot yet independently verify the reported attacks against current CALEA intercept devices, we can verify that attacks against software with similar network analysis functionality have been very successful. What's more, devices produced by vendors who also offer intercept capabilities have had remotely exploitable vulnerabilities unrelated to those capabilities.[103] Adding surveillance capabilities to ordinary network equipment will never make the equipment more secure; at best, it may not create any new vulnerability.

V. Conclusion

[103] See, e.g., "Cisco Internet Security Advisories", available at http://www.cisco.com/warp/public/707/advisory.html (product security vulnerabilities acknowledged by Cisco Systems). Cisco has been commendably proactive about disclosure of its security vulnerabilities. Other vendors doubtless experience similar levels of vulnerability, but some may choose to conceal their vulnerabilities from the public. We do not suggest that the number of reported security flaws is a measure of the level of vulnerability that a particular vendor's products experience. We do suggest that all vendors of products with wiretapping capabilities experience significant security problems, whether they are reported or not.

EFF believes that the Commission should reject the FBI petition in its entirety and affirm Congress's plain mandate that information services are not subject to CALEA. If, however, the Commission wishes to consider the FBI petition, it should consider exercising its 47 U.S.C. § 229(a) authority to establish a process that better evaluates the public interest, including a fact-finding process that is not based merely on anecdotal evidence. We suggest that the Commission consider establishing a broadly based task force, including representatives from consumer groups and civil liberties organizations, as well as from law enforcement, the telecommunications industry, the computer hardware industry, the computer software industry and free software or open source community, computer security experts, and the consumer electronics industry to examine at least the following questions:

-- How well has CALEA worked so far?
-- Has CALEA been abused?
-- How much has CALEA cost society, and how much will its expansion cost?
-- How will CALEA affect national innovation and global competitiveness?

Respectfully submitted,

Lee Tien
Senior Staff Attorney
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
tien@eff.org
(415) 436-9333 x 102