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

REPLY COMMENTS OF ELECTRONIC FRONTIER FOUNDATION

I. The FBI's interpretation of CALEA raises substantial constitutional questions that the Commission should avoid.

In enacting CALEA, Congress recognized that "the question of whether companies have any obligation to design their systems such that they do not impede law enforcement interception has never been ajudicated."[1] That statement remains true today.

EFF believes that technological change has only made CALEA's constitutionality increasingly uncertain. As the Supreme Court recently noted, "It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology. . . . The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy."[2]

That Fourth Amendment privacy and the advance of technology are closely linked strongly suggests that the Commission should be extremely wary of interpreting CALEA expansively in the context of new technologies. CALEA was a narrowly crafted statute, enacted to address the specific law enforcement concern that wiretaps of telephone conversations were becoming more difficult with the rise of digital telephone networks. Congress expressly declined to regulate information services or to require the re-engineering of the Internet.

---

[1] H.R. Rep. 103-827(I), 103d Cong., 2d Sess. (1994), reprinted at 1994 U.S.C.C.A.N. 3489, 3493.

[2] Kyllo v. United States, 533 U.S. 27, 33-34 (2001).

EFF believes that CALEA poses at least two serious constitutional questions. The first question is whether the government may constitutionally force private actors to design their systems such that they either facilitate or do not impede governmental surveillance. The second question is whether the FBI's interpretation of CALEA, combined with changes in technology, would allow the unconstitutional collection of communications contents using tools weaker than a Title III interception order; EFF believes that it will. We focus primarily on the issue of "call-identifying information" as defined by CALEA, and its close cousin, "dialing, routing, addressing and signaling information" as defined by the pen-register/trap-and-trace statute. [3]

Accordingly, we urge the Commission to reject the FBI's petition, and to avoid endorsing in any way the FBI's overbroad interpretation of CALEA.

II. As interpreted by the FBI, CALEA may unconstitutionally impose technical design mandates for surveillance.

People have long used technology to protect their privacy. We close our doors, lower our curtains, and enclose letters within envelopes in order to make it harder for others – including law enforcement – to know about our lives. And as the seminal case of Katz v. United States[4] demonstrates, we often protect our privacy by using *others'* facilities and technology. As the Court put it:

> "a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."[5]

In this passage, the Court did not limit its understanding of the Fourth Amendment to the technology of telephony. The Court instead appealed to two distinct but important ideas: that entering a phone booth and closing the door is a social practice for protecting privacy; and that the Fourth Amendment's protections must understand the "vital role" of technology in enabling our daily private communications.

CALEA therefore raises fundamental constitutional questions: whether the government may facilitate government surveillance of our private lives by interfering with the design and use of technology so as to prevent us from taking precautionary technological measures to protect our private communications, and if so, under what level of constitutional scrutiny.

---

[3] 18 U.S.C. §3127(3).
[4] 389 U.S. 347 (1967).
[5] Id. at 352.

The recent Kyllo case[6] suggests that CALEA's design mandates may violate the Fourth Amendment. In Kyllo, the Court held that law enforcement use of a thermal imaging device that can capture heat emanating from a house constituted a Fourth Amendment "search." The Court noted that while Katz's "reasonable expectation of privacy" test may be difficult to administer, "there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*. To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment."[7] As a result, the use of the thermal imaging technology constituted a "search," at least where "the technology in question is not in general public use."[8]

Moreover, the Court rejected the government's argument that the thermal imaging did not "search" the interior of the home because it detected "only heat radiating from the external surface of the house."[9] The Court drew an analogy to the Katz case, where the eavesdropping device "picked up only sound waves that reached the exterior of the phone booth."[10] Such a "mechanical interpretation of the Fourth Amendment . . . . would leave the homeowner at the mercy of advancing technology."[11] Instead, a rule regarding advanced technologies "must take account of more sophisticated systems that are already in use or in development."[12]

CALEA's requirement that common carriers design their systems to facilitate surveillance thus conflicts with Kyllo in two ways. First, CALEA unquestionably was and is aimed at changing "the minimal expectation of privacy that exists" for communications that use telecommunications common carriers. The point of the FBI's "Digital Telephony" initiative was that the technology used by telephone companies conferred too much privacy on telephone users, and that telephone companies should be required to redesign their systems so that telephone users would have less privacy.

Second, the FBI's interpretation of CALEA ignores Kyllo's presumption that Fourth Amendment protections should take account of advancing technologies. As noted in EFF's initial comments in this docket, the notion of a "Fourth Amendment status quo" for electronic surveillance is an artificial concept. Fourth Amendment protections on the Internet should not be narrowly defined based on those that applied in the telephone context. Rather, those protections must keep pace with the development of privacy-invasive technologies, and as in Kyllo expand as necessary to counter new privacy threats.

---

[6] 533 U.S. 27 (2001).
[7] Kyllo at 34 (emphasis in original).
[8] Ibid.("This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.").
[9] Kyllo, at 35 (quoting Brief for United States 26).
[10] Ibid.
[11] Ibid.
[12] Id. at 36.

CALEA is not itself a search.[13] Rather, it is a government-mandated restriction on privacy precautions. But as a practical matter there is little difference between a search and a government action that takes away our privacy precautions. Suppose the government had responded to the decision in Katz by banning phone booth doors, thus denying persons a useful resource that could be relied upon to create a physically bounded zone of privacy. There would be little doubt that such a law would be subject to review under the Fourth Amendment. Similar examples would include laws that forbade the closing of curtains, the enclosure of letters within opaque envelopes, or the use of encryption to conceal the contents of electronic communications.[14]

III. As interpreted by the FBI, CALEA may unconstitutionally permit the collection of communications contents under a pen/trap order.

A basic rule of electronic surveillance is that the government must use a Title III order (or similar order under the Foreign Intelligence Surveillance Act) in order to obtain the contents of a communication.[15] Law enforcement may not use lesser authorization, such as a pen register or trap-and-trace order, to intercept communications contents.[16] Unfortunately, the meaning of communications contents has never been clearly defined, either by the courts or by Congress. The result has been steady erosion in privacy protections. EFF urges the Commission to refrain from exacerbating the constitutional issues posed by the blurring of the line between CII and CC.

In its 1979 Smith v. Maryland decision, the Supreme Court found that there was no constitutional privacy interest in the numbers dialed on a telephone, which was the information obtained when a pen register was installed on the defendant's telephone line. Noting that pen registers only capture the numbers dialed on a telephone, the Court found that Mr. Smith lacked both a subjective and an objective expectation of privacy in those numbers. He lacked a subjective or actual expectation of privacy because telephone users necessarily must convey dialed numbers to the telephone company. Id. at 742-43. He lacked an objective expectation of privacy under the rule that exposing information to a third party eliminates any such privacy expectation. Id. at 743. The decisive factors were

---

[13] See Kyllo, at 32, n. 1 (offering dictionary definition of "to search" as "[t]o look over or through for the purpose of finding something; to explore; to examine by inspection") (citation omitted).

[14] The Court has observed that there are situations where the standard Katz test "would provide an inadequate index of Fourth Amendment protection." Smith v. Md., 442 U.S. 735, 741 n. 5 (1979) (noting that "if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects").

[15] Title III currently defines communications "contents" to include "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

[16] 18 U.S.C. §§ 3127(3), (4) (information obtained via pen register or trap-and-trace device "shall not include the contents of any communication").

that Mr. Smith had voluntarily conveyed the information to the phone company, and that the phone company had the facilities to record it, whether or not it actually did.[17]

A. The capabilities of contemporary pen registers and trap and trace devices far exceed those contemplated in Smith v. Maryland.

Critical to the Court's decision in Smith was the fact that "pen registers do not acquire the contents of communications."[18] The Court expressly noted that

> "a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed—a means of establishing communication. Neither the purport of any communication between the caller or the recipient of the call, their identities, nor whether the call was even completed, is disclosed by pen registers."[19]

The limited nature of the pen/trap surveillance was important because at that time, Title III defined communication "contents" as including "any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of the communication."[20] Thus, pen registers and trap-and-trace devices had very limited capacities to capture information in the late 1970s,[21] and it was these limited devices that the Supreme Court found were not regulated by the Fourth Amendment.

Since that time, much has changed. In 1986 Congress in the Electronic Communications Privacy Act amended the definition of "contents" to exclude the parties'

---

[17] As numerous commentators have noted, this reasoning is circular: had the decision gone the other way, "the telephone company would not have been free to record the information, on behalf of the police, without obtaining a warrant." Susan Freiwald, at 964 n. 67; see Clifford S. Fishman, Pen Registers and Privacy: Risks, Expectations, and the Nullification of Congressional Intent, 29 Cath. U. L. Rev. 557 (1980); cf. Richard A. Posner, The Uncertain Protection of Privacy by the Supreme Court, 1979 Sup. Ct. Rev. 173, 210 n. 102 (calling Smith Court's reliance on exposure of telephone numbers a "highly artificial ground").

[18] Id. at 741.

[19] Id. at 741, quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 167 (1977).

[20] See Pub. L. No. 90-351, Title III, 802, 82 Stat. 112 (1968).

[21] See also United States v. Dote, 371 F.2d 176, 178 (7th Cir. 1966) (pen register is "a mechanical device attached on occasion to a given telephone line, usually at the central telephone offices. A pulsation of the dial on a line to which the pen register is attached records on a paper tape dashes equal to the number dialed. The paper tape then becomes a permanent and complete record of outgoing calls as well as the numbers called on the particular line. . . . There is neither recording nor monitoring of the conversation.")

identities and the communication's existence.[22] Courts, meanwhile, "have considered as pen registers devices that record the time, date and duration of both incoming and outgoing calls,"[23] as well as non-numeric caller-ID information and "other digits dialed, such as personal identification numbers used in maneuvering through voice-mail systems."[24]

In short, the power of technology to gather information about communications has increased greatly, even for plain old telephone calls. As the D.C. Circuit clearly recognized, post cut-through dialed digit extraction does not merely collect telephone numbers but also "call content," as when a person enters bank account numbers, voicemail passwords, pager messages, or prescription numbers.[25] The application of the pen register and trap-and-trace device to the Internet creates even greater privacy issues.

B. The use of pen/trap devices on the Internet further blurs the constitutional line between protected communications "content" and unprotected "transactional" information.

To the extent that the Commission tentatively interprets CALEA to apply to broadband telephony, EFF believes that monitoring packet-header information exacerbates the constitutional problems raised by broad technological design mandates for surveillance.

As Stewart Baker, former general counsel to the National Security Agency told Congress, "none of the fights with industry have been over whether the FBI can get content . . . . The fights have all turned on the FBI's efforts to get more and more transactional data under the guise of trap-and-trace devices and the like, I think because . . . the legal standards for getting that information is quite low."[26]

As we noted in our initial comments, there is far more fine-grained "transactional" information available about electronic messaging today than ever before. Furthermore, as new communications applications and protocols are developed and transactional information and communication contents become increasingly hard to distinguish, pen/trap on the Internet will become even more constitutionally problematic. Already there are two common situations where "transactional" information is indistinguishable from "content" information.

---

[22] 18 U.S.C. § 2510(8).
[23] Freiwald, at 986.
[24] Freiwald, at 987. See also U.S. v. Goodwin, 2001 WL 1863565 (E.D.Mo. 2001) and U.S. v. Harvey, 2003 WL 22052993 (E.D.Mo. 2003) (pen registers and trap and trace devices include enhanced caller identification devices).
[25] U.S. Telecom Assn. v. F.C.C., 277 F.3d 450, 462, 343 U.S.App.D.C. 278, 290 (2000)
[26] Oversight Hearing (Transcript) of the House Subcommittee on the Constitution, Fourth Amendment Issues Raised by the FBI's "Carnivore" Program (April 6, 2000), at 60.

First, some Internet "addressing" information contains content. Obvious examples include e-mail subject headers and URLs like http://www.eff.org/Privacy/Surveillance//20040413_EFF_CALEA_comments.php. Because the definition of communications "contents" includes "any information concerning the substance, purport, or meaning of that communication," capturing any of this information requires a Title III order.

Even if URLs are not directly intercepted, capturing IP addresses that correspond to web pages necessarily reveals what a person is listening to, viewing or reading. In this situation the communication is between the person and the visited webpage, such as http://www.eff.org. Even though the numeric IP address, e.g., [196.202.155.22], could be said to contain no contents, it nevertheless maps to a webpage the URL of which can be determined via the public DNS or even by simply going to that webpage.

In short, allowing the capture of such IP addresses would subvert the requirement of a Title III intercept order for capturing communications contents. Clearly, law enforcement may with a proper showing obtain valid Title III order to intercept a surveillance target's communications, such as those with websites. Yet a pen/trap order that allowed law enforcement to collect the URLs or IP addresses of those websites would give law enforcement the functional equivalent of a Title III interception – law enforcement would know what pages had been accessed.

CALEA's legislative history does not make clear how the notion of CII should be applied in the Internet context. When CALEA was debated, the FBI stated that CII would include "a datagram, that identifies the origin and destination of the communication. For data services, this information is typically the source (calling) address and destination (called) address contained in fields of the data unit, such as the header of a frame or packet."[27]

Precisely what this means is unclear, however, because of the use of encapsulation on the Internet. Different "layers" (such as the link, network, transport, and application layer) use different addresses. When Ethernet is used, the link layer addresses are the device or MAC addresses of the Ethernet devices used. An address like "00:02:E3:10:86:F3" (the link layer address of the machine that gets e-mail for EFF) is CII within the link layer. The network or IP layer uses source and destination IP addresses. When e-mail is sent to anyone at EFF, the destination IP address is the EFF mail server, 209.237.229.14 – which does not identify anyone personally. Port numbers (like TCP port 25, commonly used for e-mail) are addressing information at yet another layer, the transport layer, while email addresses are addressing information at the application layer.

Given the constitutional backdrop of Smith's limited approval of pen registers and trap-and-trace devices in the circuit-switched telephone network, there is no clear constitutional basis for permitting such devices to capture any information beyond the "means of establishing communication" in packet-switched electronic communications

networks. In the Internet context, this means that at most only the network layer transactions and source and destination IP addresses should be treated as the functional equivalent of telephone numbers, and only to the extent that those IP addresses do not map directly to a particular web page.

IV. Conclusion

The FBI's proposed rules regarding CALEA implementation, in addition to going far beyond Congress' intent when enacting the statute (as described at length in our previous comments), poses serious constitutional questions that the Commission would do best to avoid. To the extent that the petioners' CALEA interpretation may authorize the FBI to unconstitutionally disarm the public of the ability to take privacy precautions when communicating over the Internet, or may allow the FBI to intercept communications content without the constitutionally required Title III order, the Commission should in its discretion leave such questions to Congress and the judiciary and refrain from additional rulemaking.

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