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

In the Matter of	)	
	)	ET Docket No. 04-295
Communications Assistance for Law Enforcement	)	RM-10865
Act and Broadband Access and Services	)	
	)	

REPLY COMMENTS OF THE ELECTRONIC FRONTIER FOUNDATION

Lee Tien, Esq.
Kurt Opsahl, Esq.
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333

December 21, 2004

I. INTRODUCTION

The Electronic Frontier Foundation ("EFF")[1] respectfully submits these reply comments in the above-referenced matter. EFF continues to oppose the tentative rules proposed by the Federal Communications Commission ("FCC") in the Notice of Proposed Rulemaking and Declaratory Ruling ("NPRM"), released August 9, 2004.

These reply comments supplement and expand upon some points raised by the Joint Reply Brief of Industry and Public Interest (which EFF joined) and addresses two serious Constitutional questions raised by the Communications Assistance for Law Enforcement Act ("CALEA")[2] and the NPRM.

II. THE FCC MUST PROTECT THE PUBLIC INTEREST

Before the FCC can expand CALEA pursuant to the Substantial Replacement Clause,[3] it must determine that it is in "the public interest to deem such a person or entity to be a telecommunications carrier for purposes of this title."[4]

A. Privacy is a Critical Public Interest that the FCC Must Consider

In addition to the three specific factors identified in the legislative history of CALEA,[5] the FCC must balance the government's interest in surveillance with the public's interest in protecting "privacy in the face of increasingly powerful and personally revealing technologies."[6]

The Comment of the United States Department of Justice (filed Nov. 8, 2004) ("DOJ Comment") agrees: "The Commission should consider the three factors

---

[1] The Electronic Frontier Foundation is the leading civil liberties organization working to protect rights in the digital world. Founded in 1990, EFF actively encourages and challenges industry and government to support free expression and privacy online. EFF is a member-supported organization and maintains one of the most linked-to websites in the world at <http://www.eff.org/>.

[2] Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat. 4279 (1994), codified in Title 47, United States Code Sections 1001 to 1021.

[3] 47 U.S.C. § 1001(8)(B)(ii).

[4] 47 U.S.C. § 1001(8)(B)(ii).

[5] H.R. Rep. No. 103-827, 103d Cong., 2d Sess., pt. 1, at 21 (1994), reprinted in 1994 U.S.C.C.A.N. 3489 ("House Report") (the three factors are to "promote competition, encourage the development of new technologies, and protect public safety and national security.")

[6] *Id*. at 13, 22.

enumerated in the House Report's section-by-section analysis of that provision as well as the extent to which a public-interest determination would serve the privacy interests that CALEA was intended to protect."[7] EFF agrees that the FCC's public interest determination must include the privacy interests, but disagrees strongly with the DOJ's argument on how CALEA and its expansion to the Internet might effect privacy.

Essentially, the DOJ argues that CALEA is protective of privacy because "Service providers that have deployed CALEA capabilities are better able to comply fully with court intercept orders by delivering to law enforcement only the information authorized in the order."[8] Put another way, the DOJ argues that CALEA can help privacy by minimizing overly broad requests.

The DOJ fails to acknowledge that broadband Internet access providers and managed VOIP providers are already able to protect users from overly broad requests without CALEA assistance requirements.[9] More importantly, any privacy benefits of assistance capabilities are outweighed by the security holes introduced. Indeed, the NPRM will reduce user privacy if there are more taps (or pen register orders or trap-and-trace orders) because surveillance becomes cheaper. Furthermore, the public interest in protecting privacy cannot be served by promoting a legal norm of mandated tappability.

B. The FCC Must Consider the Public Interest in Innovation

CALEA's legislative history also requires the FCC to consider whether the application of the Substantial Replacement Clause would act to "encourage the development of new technologies," and balance the government's interest in surveillance with the public's interest in avoiding "impeding the development of new communications services and technologies."[10]

---

[7] DOJ Comment at 16.

[8] DOJ Comment at 19.

[9] Indeed, such companies have legal obligations not to provide certain information to the government absent appropriate legal process. *See e.g.* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

[10] House Report at 13, 21-22.

1. Lack of Regulation Can Provide "Regulatory Certainty" and Also Promote Innovation

The DOJ Comment argues that "encouraging the development of new technologies includes promoting regulatory certainty."[11] From this premise, the DOJ makes the unsupported logical leap to conclude that the public interest in innovation is best served by government design mandates imposed upon all manufacturers and telecommunications carriers. As an initial matter, the history of CALEA implementation is replete with regulatory uncertainty, leading to litigation and FCC proceedings to clarify the statute, and there is no evidence that expanding the reach of CALEA will promote regulatory certainty.[12]

Furthermore, the DOJ Comment fails to note that regulatory certainty can just as easily be provided by lack of regulations – as new technologies and services are developed and deployed, innovators would know *not* to include CALEA capabilities. Not only would this provide the regulatory certainty that the DOJ argues will assist innovation, the companies can avoid the need to design in accordance with government specifications, freeing the technologies to develop unimpeded.

2. DOJ's Definition of "Reasonably Available" Will Harm Innovation

As argued by the DOJ Comment, "any definition of 'reasonably available' should be based on the technical solutions a carrier and vendor can achieve when they first design the network, not on the unfortunate realities that prevail after a non-compliant network has already been constructed."[13] Specifically, the DOJ envisions a future in which "carriers should first seek any needed clarification of their CALEA obligations and then proceed to design their networks."[14]

---

[11] DOJ Comment at 17 (emphasis removed).

[12] *See generally* James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 Alb. L.J. Sci. & Tech. 65 (1997)

[13] *Id.* at 45.

[14] *Id.* at n.148.

Requiring technology companies to seek prior approval for network design, whether in the form originally proposed in the FBI Joint Petition[15] or through the imposition of a backward looking definition of "reasonably available," will substantially harm innovation.[16] Innovators would need to be circumspect (and/or obtain expensive legal advice) in the initial stages of development for fear that a court could later determine that they could have achieved a technical solution on initial design. The dynamic effect would be for the government to get inextricably involved earlier in the design process, advising innovators on what 'could be achieved.' Not only will this slow the time-to-market for new products, it will restrict development of strong privacy protections in network design, and/or encourage innovators to move to a less regulatory environment.

3. Open Source Projects Must Be Protected from Onerous CALEA Compliance Requirements

As discussed at length in the comments of EFF and others to date, the proposed definition of "switching" is overly broad and at odds with the intent of Congress in enacting CALEA.[17] The even broader definition promoted in the DOJ Comments, "anything that can be characterized as switching,"[18] also opens the possibility that open source developers who provide Internet service providers with software that has "addressing and intelligence functions for packet-based communications" might now be considered telecommunications support services.[19] This could effect significant open source projects: For example, the Linux operating system's kernel includes routing functions, and any firewall software program will perform addressing or intelligence

[15] Joint Petition for Expedited Rulemaking, filed by the U.S. Department of Justice, the Federal Bureau of Investigation, and the Drug Enforcement Administration ("FBI Joint Petition").

[16] House Report at 19.

[17] NPRM ¶ 43 ("switching includes the use of "routers, softswitches, and other equipment that may provide addressing and intelligence functions for packet-based communications to manage and direct the communications along to their intended destinations.")

[18] DOJ Comment at 9.

[19] *See* NPRM ¶ 48 ("broadband Internet access includes the switching (routing) … functionality") and Section 102(7) ("'telecommunications support services' means a ... software ... used by a telecommunications carrier for ... switching functions").

functions.[20] "Most Unix-like operating systems include all necessary software to perform routing; the Linux Router Project is an example of a Linux distribution that specialises in routing."[21]

Furthermore, if an open source project falls under the requirements of Section 106(b), it must "on a reasonably timely basis and at a reasonable charge, make available to the telecommunications carriers using its [software] such features or modifications as are necessary to permit such carriers to comply [with CALEA]."

EFF believes that this potential application of CALEA to open source software shows the failure of the NPRM's definitions: CALEA was never intended to reach Linux, a popular open source operating system used by enterprises large and small, but which also happens to provide routing functions.

III. THE NPRM HAS SEVERE CONSTITUTIONAL INFIRMITIES

As discussed in detail in EFF's Reply Comments to the FBI Joint Petition underlying this rulemaking,[22] the FBI's proposal raised severe 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 proposed rule, combined with changes in technology, would allow the unconstitutional collection of communications contents using tools weaker than a Title III interception order.[23] Both the NPRM and the DOJ Comment fail to resolve these questions. EFF incorporates its earlier Reply Comments by reference.

---

[20] *See* <http://en.wikipedia.org/wiki/Linux> ("A number of network firewalls and routers, including several from Linksys, use Linux internally, due to its advanced firewalling and routing capabilities.").

[21] <http://en.wikipedia.org/wiki/Router> (also listing manufacturers of routers and routing software projects).

[22] Available from the FCC docket at <http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6516182047>.

[23] Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 212 (1968) ("Title III").

A. The NPRM May Unconstitutionally Impose Technical Design Mandates for Surveillance

As the seminal case of *Katz v. United States* demonstrates, we often protect our privacy by using others' facilities and technology.[24] 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.

Kyllo v. United States[25] suggests that CALEA's design mandates may violate the Fourth Amendment. CALEA's requirement that telecommunications carriers design their systems to facilitate surveillance 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.

Second, 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.

Accordingly, to the extent that the FCC's final rule in this matter mandates restrictions on privacy precautions, it will impermissibly conflict with the Constitution.

B. The NPRM 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.[26] Law enforcement may not use lesser authorization,

---

[24] *Katz v. United States,* 389 U.S. 347 (1967).

[25] 533 U.S. 27 (2001).

[26] 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).

such as a pen register or trap-and-trace order, to intercept communications contents.[27] Unfortunately, the meaning of communications contents has never been clearly defined, either by the courts or by Congress. As the NPRM recognized, the meaning of the term "call-identifying information" is unclear in the Internet context.[28] The result of this lack of clarity has been steady erosion in privacy protections. The NPRM exacerbates the constitutional issues posed by the blurring of the line between CII and communications contents.

In its 1979 *Smith v. Maryland* decision, the U.S. 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.[29] 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.[30] He lacked an objective expectation of privacy under the rule that exposing information to a third party eliminates any such privacy expectation.[31] The decisive factors were 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.

The application of the pen register and trap-and-trace device to the Internet creates even greater privacy issues because the capabilities of contemporary pen registers and trap and trace devices far exceed those contemplated in *Smith v. Maryland*. Monitoring packet-header information exacerbates the constitutional problems raised by broad technological design mandates for surveillance.

---

[27] 18 U.S.C. §§ 3127(3), (4) (information obtained via pen register device "shall not include the contents of any communication").

[28] NPRM ¶¶ 66-67. The DOJ and FBI have done nothing to clarify what CII will mean. *See generally* Joint Reply Comments of Industry and Public Interest, Section II (filed Dec. 21, 2004).

[29] *Smith v. Maryland* , 442 U.S. 735 (1979).

[30] *Id*. at 742-43.

[31] *Id*. at 743.

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 NPRM, in addition to going far beyond Congress' intent when enacting the statute (as described at length in EFF's previous comments), does not serve the public interest and poses serious constitutional questions that the FCC would do best to avoid. EFF urges the FCC to abandon the NPRM in its entirety and affirm Congress's plain mandate that information services, including broadband Internet access providers and VOIP providers, are not subject to CALEA.

Respectfully submitted,

Lee Tien, Esq.
Kurt Opsahl. Esq.
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333

December 21, 2004