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	)	
	)	

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

November 8, 2004

TABLE OF CONTENTS

I. SUMMARY 1

II. BACKGROUND 2

III. THE FCC HAS RECEIVED NO EVIDENCE THAT THIS RULEMAKING IS NECESSARY 4

A. The FBI Already Has the Necessary Tools 5
B. The NPRM is Not Supported By Particularized Facts 7

IV. THE NPRM CONFLICTS WITH CALEA 8

A. Congress Intended CALEA to be Narrowly Construed 8
B. The NPRM's Substantial Replacement Clause Analysis is Flawed 9
C. CALEA Specifically Excludes Information Services 12
D. The NPRM's Definitions Are Overly Broad. 15
E. Section 151 Cannot Save the NPRM 17

V. THE NPRM IS NOT IN THE PUBLIC INTEREST 18

A. The NPRM Imposes Risks to Security 18
B. The NPRM Poses a Risk to Innovation 22
C. The NPRM Poses a Risk to Privacy 23

THE "TRUSTED THIRD PARTIES" MODEL IS NOT APPROPRIATE 25

A. Abdication of Traditional Government Function 25
B. The FCC Will Create a Surveillance-Industrial Complex 26

CONCLUSION 27

A. Drop the NPRM Altogether 27
B. Alternative: Establishing a CALEA Task Force 27

I. SUMMARY

The Electronic Frontier Foundation ("EFF")[1] respectfully submits these comments in the above-referenced matter. EFF generally opposes the tentative rules proposed by the Federal Communications Commission ("FCC") in the Notice of Proposed Rulemaking and Declaratory Ruling ("NPRM"), released August 9, 2004.[2]

Based on an insufficient record, the NPRM proposes to rewrite the Communications Assistance for Law Enforcement Act ("CALEA"),[3] fundamentally altering its scope and meaning, going far beyond the narrowly construed statute Congress intended. There is no rational connection between the record and the proposed rule because law enforcement agencies have failed to provide evidence of a problem that needs to be resolved. To the contrary, law enforcement already has the online surveillance tools it needs

Even if there were a record upon which to consider a rulemaking, the proposed rules cannot be supported by the statute. The NPRM essentially suggests that CALEA, which Congress intended to apply only to the phone system, should also apply to the Internet. Relying upon a flawed interpretation of the Substantial Replacement Clause, the NPRM relegates Congress' exclusion of the Internet to so much spilt ink and abandons the particularized analysis needed to find a specific person or entity provides a service that acts as a substantial replacement of the local telephone exchange in a particular state. The NPRM instead applies a functional analysis whereby any service that arguably replaces any portion of the prior telephony regime must look down the barrel of CALEA compliance. This is contrary to both the plain language and legislative history of the statute.

---

[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] EFF agrees with the NPRM's rejection of "Law Enforcement's proposal regarding the identification of future services and entities subject to CALEA," NPRM ¶ 60, but notes that the overall rules proposed in the NPRM would have an equally harmful effect on security, innovation and privacy.

[3] 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.

Furthermore, the NPRM's tentative rules fail to balance the three key purposes of CALEA, choosing law enforcement's interest in surveillance over the public's interest in privacy and innovation. Yet these interests cannot be ignored. The application of CALEA to Internet communications might backfire: many of the technologies currently used to create wiretap-friendly computer networks make the people on those networks more vulnerable to attackers who want to steal their data or personal information, threatening both privacy and security. At the same time, the burdens of CALEA compliance will stifle technological innovation and push development of new Internet communications tools and services overseas, outside the FCC's regulatory ambit.

EFF therefore recommends that the FCC withdraw the NPRM and leave it Congress to decide whether to expand CALEA beyond its current scope.

II. BACKGROUND

The FCC has recognized that when Congress enacted CALEA ten years ago in October 1994, the legislature

> 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.[4]

In this age of rapid technological innovation, however, ten years is a long time. CALEA was already showing is age in 1999, when the FCC 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").[5] The JEM Report, submitted to the FCC in September 2000, made clear that

---

[4] *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 ("House Report")); *see also* NPRM ¶ 3 and n.4.

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

packet-mode technologies raised serious legal, as well as technical, issues. For example, it found that the crucial statutory phrase "call-identifying information"[6] was "ambiguous with regard to packet communications," and that the TIA experts "could not define 'call-identifying information' for packet services."[7] 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."[8]

The problems of forcing CALEA requirements upon new technologies and a constantly changing communications system are even greater today than when examined in 1999. 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 technological innovation, attempting to apply CALEA to the Internet creates enormous legal, technical, economic and social problems.

Nevertheless, on March 10, 2004, the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), and the Drug Enforcement Administration (DEA) (collectively FBI) filed a joint petition[9] requesting that CALEA's reach be expanded to cover communications that travel over the Internet. The FCC responded with the NPRM, which expands the reach of CALEA by redefining what constitutes a "substantial replacement" of the telephone service, tentatively concluding that broadband Internet

---

[6] 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").

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

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

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

access providers[10] and managed Voice Over Internet Protocol ("VOIP")[11] substantially replace a portion of the functionality of local exchanges, and therefore are subject to the requirements of CALEA. As explained below, the NPRM's redefinition is neither warranted by the record, consistent with the statutory text nor in the public interest.

III. THE FCC HAS RECEIVED NO EVIDENCE THAT THIS RULEMAKING IS NECESSARY

The FCC should defer to Congress because the FCC does not have sufficient information to support a rulemaking. Before the FCC can issue a Final Rule, it must "examine the relevant data and articulate a satisfactory explanation for its action including a rational connection between the facts found and the choice made."[12] Here, the record contains 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, a small percentage of the total number of electronic surveillance orders issued in that period.[13] Moreover, the public record merely indicates that law enforcement could not "fully" implement authorized electronic surveillance.[14] The FBI did not assert that these problems materially affected the ability of law enforcement agencies to investigate crime.

The current record also contains no evidence that today's communications system materially affects law enforcement's ability to investigate crime. The FBI petition asserts that: "critical electronic surveillance is being compromised today by providers who have

---

[10] Defined as all "facilities-based providers of any type of broadband Internet access service." NPRM ¶ 37.

[11] (Defined as "providers of managed VOIP services, which are offered to the general public as a means of communicating with any telephone subscriber, including parties reachable only through the PSTN." NPRM ¶ 56. The NPRM does not directly define "managed," adopting the FBI Petition's description of "those services that offer voice communications calling capability whereby the VOIP provider acts as a mediator to manage the communication between end points and to provide" call management information.

[12] *Motor Vehicle Manufacturers Ass'n v. State Farm Mutual Auto. Ins. Co.*, 463 U.S. 29, 43 (1983) (internal quotation marks omitted).

[13] House Report at 15. It is not clear from the legislative history whether these problems were encountered in one year or over several years.

[14] *Id.* at 14.

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.[15] Yet, no evidence supports these assertions.

Similarly, the FCC has been presented with no evidence that such problems materially affect criminal investigations. We do not know, for instance, whether law enforcement is able to gather necessary evidence through its existing surveillance authority.[16] We do know that law enforcement authority to conduct electronic surveillance as well as to obtain records has increased dramatically since 1994.[17] For example, the requirements for conducting "roving wiretaps" under Title III were significantly relaxed even before the enactment of the PATRIOT Act, and the PATRIOT Act further relaxed restrictions on law enforcement authority for interceptions and pen register and trap-and-trace ("pen-trap") surveillance.[18] Yet law enforcement has failed to provide any evidence showing that their expanding arsenal of electronic surveillance tools is inadequate.

A. The FBI Already Has the Necessary Tools

Before issuing a Final Rule, the FCC must require a record that demonstrates that law enforcement is worse off today under an honestly defined status quo—one not limited to areas that the FBI deems a problem. The FBI cannot, because it already has the necessary tools to conduct lawful surveillance. Indeed, there is evidence that law enforcement has had little problem with Internet interceptions.[19]

---

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

[16] It is not disputed that the FBI has the legal authority to conduct surveillance on the Internet in appropriate circumstances regardless of the FCC's interpretation of CALEA. *See e.g.* Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 212 (1968) ("Title III"), the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) ("ECPA"), and the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801-1843 ("FISA").

[17] 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).

[18] *See* USA PATRIOT Act of 2001, Pub. L. 107-56, 115 Stat. 272 (2001).

[19] *See* "Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications," (April 30, 2004), available at <http://www.uscourts.gov/wiretap03/contents.html>.

The FBI has demonstrated considerable ability to adapt to new technologies on its own. The FBI's "Carnivore" technology enables the broad interception of packet-mode information, and even end-user encryption—expressly permitted by CALEA—does not appear to have materially affected the ability to conduct surveillance, given the FBI's technical creativity in using key loggers.[20]

Indeed, 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,[21] while data aggregators like ChoicePoint possess vast records of personal information that the FBI uses.[22] Simply put, more records are more cheaply available than ever before, making subpoenas and records searches a far more useful law enforcement technique.

To the extent that the FBI believes that a telecommunications carrier has not met its CALEA obligations in assisting with a court order for electronic surveillance, it can seek a court order to compel the carrier to comply.[23] 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.[24] Moreover, nothing bars the FBI from petitioning the FCC for a ruling that CALEA's assistance requirements are "reasonably achievable" for any equipment, facilities or services installed or deployed after 1995.[25] Considering this vast array of tools and remedies, the NPRM is simply unnecessary.

---

[20] *See* 47 U.S.C. § 1002(b)(3); *see also United States v. Scarfo*, 180 F.Supp.2d 572, 581 (D.N.J. 2001) (FBI installed a "key logger" on a suspect's computer in order to capture the suspect's PGP encryption passphrase.)

[21] Dempsey, *supra* note 17, at 82.

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

[23] 18 U.S.C. § 2522(a).

[24] 18 U.S.C. § 2522(b)

[25] 47 U.S.C. § 1008(b) provides that "a telecommunications carrier or any other interested person" may petition the FCC for such a ruling.

B. The NPRM is Not Supported by Particularized Facts

The Substantial Replacement Clause, Section 1001(8)(B)(ii), is clear: the FCC is only empowered to find a particular "person or entity" provides a service that is replacing "a substantial portion of the local telephone exchange service."[26] Yet the NPRM instead proposes to apply CALEA to categories of broadband Internet access services and managed VOIP, without identifying facts associated with particular persons or entities.[27]

A Final Rule cannot be made without an appropriate record. It is mere speculation to claim that any of these broadband services is a substantial replacement for local exchange service. The FBI Petition claims that broadband use is "surging,"[28] 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."[29] But it does not say that the percentage of local exchange service within a state replaced by any service is "substantial."

Furthermore, there is no record on the effect of the NPRM on the public interest, even though the Substantial Replacement Clause requires the FCC to develop and analyze such a record prior to determining that any persons or entities qualify as a replacement.

The NPRM instead incorrectly attempts to turn the particularized analysis required by the Substantial Replacement Clause on its head, requesting comments on "discrete groups of entities for which the public interest may not be served by including them under the Substantial Replacement Provision."[30] If the NPRM's understanding of the Substantial Replacement Clause is adopted as a Final Rule, the analysis required by

---

[26] 47 U.S.C. § 1001(8)(B)(ii); *see also* House Report at 20-21 ("FCC is authorized to deem other persons and entities to be telecommunications carriers ... to the extent that *such* person or entity serves as a replacement...") (emphasis added).

[27] *See* NPRM ¶ 37.

[28] FBI Petition at 18, n.40 ("both industry and trade press reports confirm that broadband use is surging").

[29] FBI Petition at 19, n.41 (citations omitted).

[30] NPRM ¶ 49.

CALEA to reach a substantial replacement determination will be further thwarted, as specific companies will need to petition the FCC for an exemption.[31]

Rather than placing the burden on potentially affected services, the FCC itself must particularly analyze the facts supporting a finding of Substantial Replacement by a particular person or entity and the public interest impact of such a finding. The NPRM's functional analysis is wholly lacking the particularized analysis required by CALEA,

IV. THE NPRM CONFLICTS WITH CALEA

The FCC is charged with interpreting the application of CALEA, not rewriting the statute. The NPRM gives a narrow statute addressing the needs of law enforcement in the telephone context a new interpretation inconsistent with its plain meaning. It unjustifiable broadens the reach of the Substantial Replacement Clause while defining "telecommunications carriers" in a manner inconsistent with the long-standing definition in the Communications Act. As explained below, the legislative history and the language of the statute both contradict the proposed rules in the NPRM.

A. Congress Intended CALEA to be Narrowly Construed

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 that "[t]he goal of the legislation, however, is not to reverse those industry trends,"[32] and rejected earlier proposals that CALEA be applied to Internet services.[33] For example, Congress expressly noted that "from a privacy standpoint . . . the scope of the legislation has been greatly narrowed."[34] "Earlier digital telephony proposals covered all providers of electronic communications services, which meant every business and institution in the

---

[31] *See* NPRM ¶ 61.

[32] House Report at 14.

[33] *See* House Report at 20; *see also* draft telephony bill, available at <http://www.eff.org/Privacy/Surveillance/CALEA/digtel92_bill.draft>.

[34] House Report at 18.

country. That broad approach was not practical. Nor was it justified to meet any law enforcement need."[35]

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."[36] Furthermore, courts

> 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.[37]

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."[38]

B. The NPRM's Substantial Replacement Clause Analysis is Flawed

Under CALEA's definitions, if one is "engaged in providing information services," then one is absolutely not a "telecommunications carrier."[39] A telecommunications carrier is defined as "a person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire," and

---

[35] *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.").

[36] *Id.* at 19.

[37] *Ibid.*

[38] *Id.* at 23.

[39] 47 U.S.C. § 1001(8)(C)(i).

specifically excludes "persons or entities insofar as they are engaged in providing information services."[40]

To get around this hurdle, the NPRM engages in a tortured stretch of the Substantial Replacement Clause. Essentially, the NPRM reads 'substantial' out of the clause, finding it means "any" portion, and suggesting that broadband replaces that "portion" where home computer users previously connected to their ISPs via POTS.[41] Furthermore, the NPRM interprets CALEA to mean that where a service provider falls within the Substantial Replacement Clause, it can no longer qualify for the "information services" exemption.[42]

As explained below, the plain meaning of CALEA and the legislative history shows that the NPRM's interpretation of the statute is unsupportable.

1. The Plain Meaning of CALEA Does Not Support the NPRM

The plain meaning of "a replacement for a substantial portion of the local telephone exchange service" is that CALEA will apply to an entity only if it has replaced a significant percentage of local phone service in the relevant state's market.[43] For example, if Company X's services were used by 70% of the Alaskan residents to make telephone calls, Company X would have replaced a substantial portion of the Alaskan local telephone exchange service.[44] However, simply being a substitute for some portion of the subscriber's prior service would be insufficient.

Furthermore, the Information Services Exclusions, which specifically and categorically exclude "information services" from the reach of CALEA, present no "irreconcilable tension" with the remainder of the statute, as asserted in the NPRM.[45] Under the clearest reading of the statute, Congress designed Section 1001(8)(B)(ii) (the

---

[40] *Ibid.*

[41] NPRM ¶ 44.

[42] *Id.* at ¶ 50.

[43] *See also In the Matter of Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, Second Report and Order, 15 FCC Rcd 7105 (2000), at 7118, ¶ 23.

[44] For this example, presume that Company X is not an information service under Section 1001(6) nor already a telecommunications carrier under Section 1001(8)(A) because it is not a common carrier for hire.

[45] NPRM ¶ 50.

Substantial Replacements Clause) as an expansion of subsection (8)(A) (the definition of "telecommunications carrier"), both of which are limited by the Information Services Exclusion in subsection (8)(C).

Indeed, if the NPRM's "tension" analysis were correct, it would lead to an absurdity. Section 1001(8)(C)(ii) allows the FCC, in consultation with the Attorney General, to exempt "any class or category of telecommunications carriers."[46] Yet, under the NPRM's "tension" analysis, subsection (8)(C) does not apply if an entity is defined as a telecommunications carrier pursuant to the earlier provisions of subsection (8). It is nonsensical for Congress to have granted the FCC an impotent power to exempt telecommunications carriers.

Finally, the NPRM's contention that when "a service provider is determined to fall within the Substantial Replacement Provision, by definition it cannot be providing an information service" is unsupportable because it conflicts with the statutory definition of "information services" in Section 1001(6). CALEA does not offer the FCC any authority to restrict the statutory definition of "information service," and the statute's plain language cannot be superseded by the NPRM's citation to a vaporous "tension."

Accordingly, CALEA's plain language contradicts the interpretation in the NPRM.

2. The Legislative History Clarifies "Substantial Replacement"

To the extent that the language could be considered ambiguous, the legislative history clarifies its application. As explained by Congress, the FCC's authority is limited to the power "to deem other persons and entities to be telecommunications carriers subject to [CALEA] to the extent that such person or entity serves as a replacement for the local telephone service to a substantial portion of the public within a state."[47]

This requires the FCC to look at particular persons or entities, and, with respect to that particular entity, determine whether a "substantial portion of the public within a state" is using that service as a replacement of the local telephone exchange. As noted

[46] 47 U.S.C. § 1001(8)(C)(ii).

[47] House Report at 20-21.

above, the record is absolutely devoid of evidence that any particular services meet this test.

Furthermore, the NPRM's reading of "a substantial portion of the local telephone exchange service" to be a functional reference to the replacement of any "functionality" for which telephones have ever been used is unsupportable.[48] First of all, the phrase "of the public" in the legislative history clarifies that "substantial portion" means a substantial percentage of the public uses the service as a replacement. Secondly, the "within a state" language in the legislative history is nonsensical under the functionality analysis, and can only be understood to mean the actual replacement for all aspects of local exchange service in a particular state.

Section 332 of the Communications Act can also help provide an understanding of the "substantial portion of the public within a state" language in the CALEA legislative history. In Section 332(c)(3)(A)(ii), Congress allowed states to regulate mobile services if "such service is a replacement for land line telephone exchange service for a substantial portion of the telephone land line exchange service with such State."[49] This provision tracks the legislative history language, but more clearly indicates that, like the Substantial Replacement Clause, Congress intended replacement only when a significant percentage of consumers in a state were using the alternate service instead of the local telephone exchange.

C. CALEA Specifically Excludes Information Services

Section 1001(8)(C)(i) explicitly directs the FCC not to apply CALEA to information service providers, and not to treat information service providers as telecommunications carriers.[50] "The definition of telecommunications carrier does not include persons or entities to the extent they are engaged in providing information

---

[48] NPRM ¶ 44 (the Substantial Replacement Clause reaches the "replacement of any portion of an individual subscriber's functionality previously provided via POTS...")

[49] 47 U.S.C. § 332(c)(3)(A)(ii). Likewise 47 U.S.C. § 332(d)(3) clarifies that the "substantial portion" analysis references a percentage of the public.

[50] 47 U.S.C. § 1001(8)(C)(i).

services, such as electronic mail providers, on-line services providers, such as Compuserve, Prodigy, America-On-line or Mead Data, or Internet service providers."[51]

Section 1002(a) sets forth telecommunications carrier's assistance capability requirements, and Section 1002(b)(2)(A) clarifies that any service that meets the definition of an "information service" need not comply with those requirements. Thus, Section 1002(b)(2)(A) separately excludes information services, even if provided by an entity subject to CALEA as a telecommunications carrier. Under the plain language of the statute, even if a particular entity is determined to be telecommunications carriers under the Substantial Replacement Clause, the assistance capability requirements do not apply to any "information services" provided.

CALEA capability requirements simply "do not apply to information services, such as electronic mail services, or on-line services, such as Compuserve, Prodigy, America On-line or Mead Data, or Internet service providers," as Congress explained and courts have found.[52] In particular, the Ninth Circuit clarified in *Brand X Internet Services v. FCC,*[53] that under the virtually identical definition of "information services" in the Telecommunications Act, broadband Internet access services could constitute both an information service and a telecommunications service to the end user.[54] While the FCC has sought certiorari, unless the Supreme Court reverses, *Brand X* shows that CALEA cannot reach broadband Internet access providers to the extent they function as an information service.

The Information Service Exclusions make sense in the statutory scheme because Congress envisioned these exclusions as broadly construed provisions, expanding to fit the ever-changing nature of information services. "It is the Committee's intention not to limit the definition of 'information services' to such current services, but rather to

---

[51] House Report at 20.

[52] *See id.* at 23; *see also United States Telecom Ass'n v. FCC*, 227 F.3d 450, 455 (D.C. Cir. 2000).

[53] *Brand X Internet Services v. FCC*, 345 F.3d 1120 (9th Cir. 2003).

[54] *See* 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.").

anticipate the rapid development of advanced software and to include such software services in the definition of 'information services.'"[55]

CALEA was a narrow statute, designed to address a limited issue. The Information Services Exclusions, on the other hand, were designed to expand with the development of technology, and ensure that the innovation on the Internet was not stifled by the burden of CALEA compliance.

Broadband Internet Access is an Information Service

Pursuant to 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,"[56] and expressly includes "electronic messaging services."[57] Clearly, a cable operator providing Internet access via high-speed cable modem service is not acting as a "carrier;" the FCC has found that cable operators acting in that role are information service providers.[58] Given that both wireline and cable-modem broadband access services are "information services" under the Telecommunications Act,[59] all broadband access service generally is appropriately classified as an "information service."[60]

2. Voice Over Internet Protocol is an Information Service

While the NPRM considers Vonage to be a managed VOIP provider, and therefore subject to CALEA, one district court found that Vonage is also an information

---

[55] House Report at 22.

[56] 47 U.S.C. § 1001(6)(A).

[57] 47 U.S.C. § 1001(6)(B)(iii).

[58] *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).

[59] *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.

[60] "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).

service.[61] Similarly, while the NPRM considers services such as Pulver.com's Free World Dialup, to be unmanaged VOIP not subject to CALEA, it is the software application for an information service.[62] Likewise, Skype is an application for an information service, just as Qualcomm's Eudora is an end-user application for e-mail communication.[63]

While both the *Vonage* and *Pulver.com* 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.[64] Internet telephony services not only provide standard telephony features like call forwarding and call return but use the Internet to enhance these standard features: one can listen to one's voice mail by visiting a Web page or via e-mail with sound attachments. Accordingly, under CALEA, VOIP services should be classified as "information services," whether managed or not.

D. The NPRM's Definitions Are Overly Broad.

The NPRM tentatively determines that all "facilities-based providers of any type of broadband Internet access service" are subject to CALEA, including "wireline, cable modem, satellite, wireless and broadband access by powerline."[65] Broadband is defined as over 200 kbs downstream.[66] By "facilities-based" the NPRM refers to "entities that

---

[61] *Vonage Holdings Corp. v. Minn. P.U.C.*, 290 F.Supp.2d 993, 1001 (D.Minn. 2003); *see also* NPRM at n.149.

[62] *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 (Feb. 19, 2004).

[63] The NPRM notes that it "does not propose attaching CALEA obligations to services or applications that 'ride over' the underlying broadband transmission," presumably under the Information Services Exclusions. NPRM ¶ 51. VOIP applications should also be excluded because they "ride over" Internet transmissions.

[64] House Report at 21.

[65] NPRM ¶ 37.

[66] NPRM ¶ 35.

provide transmission or switching over their own facilities between the end user and the Internet Service Provider."[67] The FCC broadly interprets "switching" to "include routers, softswitches, and other equipment that may provide addressing and intelligence functions."[68]

Under these overly broad definitions, law enforcement may one day argue that even home users or small businesses with open wireless 802.11 routers operate a user-owned "switching" facility and are therefore subject to CALEA.[69] The root of the problem is stretching CALEA's use of "switching and transmission" to refer to routers and other common networking devices. The NPRM, while acknowledging that "equipment that provides addressing or intelligence functions may not technically be switching or transmission equipment," includes in its interpretation of "switching" any device that used in "packet-based communications to manage and direct the communications along to their intended destinations."[70] Congress simply did not intend CALEA to cover consumer routers and hubs, which are available for less than $100 at consumer electronics stores.

Even if the definitions were appropriate, which they are not, an extension of CALEA to consumer electronics would not be in the public interest.[71] Like the "schools, libraries, hotels, coffee shops, etc." noted in Footnote 133 of the NPRM, consumers and their wireless routers should not be subject to CALEA obligations.

Likewise, broadband Internet access and VOIP services are not properly considered "switching and transmission services" subject to an extension of CALEA under the Substantial Replacement Clause. As explained above, Congress explicitly excluded information services like these from the reach of CALEA, and the FCC should

---

[67] NPRM n.79.

[68] NPRM ¶ 43.

[69] For example, EFF provides broadband access through an EFF-owned wireless router, which members of the public can use to connect to the Internet from anywhere within about a hundred feet of EFF's offices. Many individuals also leave their wireless routers open to the public.

[70] NPRM ¶ 43.

[71] *See* 47 U.S.C. § 1001(8)(B)(ii) (requiring the FCC to consider the public interest in a substantial replacement determination).

not try to get them in the back door by redefining "switching" beyond its meaning at the time of enactment.[72]

E. Section 151 Cannot Save the NPRM

The NPRM asks: "To the extent an entity is not a 'telecommunications carrier' under CALEA, is there any legal basis for exercising ancillary authority to impose some type of law enforcement assistance requirements on these entities? Section 151 of the Communications Act charges the Commission with carrying out its obligations for a number of stated purposes, including 'for the purpose of the national defense' and 'for the purpose of promoting safety of life and property.' How would the Information Services Exclusion and section 103(b)(2)(A) of CALEA impact the Commission's authority to exercise ancillary jurisdiction over non-subject entities?"

The answer lies in *FCC v. Midwest Video*, in which the Supreme Court held that rules requiring cable operators to provide equipment, facilities, and channel access to public were not reasonably ancillary to FCC's regulation of broadcast and therefore outside FCC jurisdiction.[73] In finding no ancillary jurisdiction, the Supreme Court noted that the FCC had been "directed explicitly by Sec. 3(h) of the Act not to treat persons engaged in broadcasting as common carriers."[74]

As the D.C. Circuit has said, "Contrary to the FCC's arguments suggesting otherwise, § 1, 47 U.S.C. § 151, does not give the FCC unlimited authority to act as it sees fit with respect to all aspects of television transmissions, without regard to the scope of the proposed regulations."[75] Likewise, Section 151 does not give the FCC unlimited authority without regard to the narrow scope of CALEA and CALEA's carve-out of information services. CALEA's exemptions clarify that ancillary authority is simply not

---

[72] *Compare* Harry Newton, *Newton's Telecom Dictionary* (7th ed. 1994) (definition focusing on circuit switching) *with* Harry Newton, *Newton's Telecom Dictionary* (19th ed. 2003) (cited in Footnote 103 of the NPRM for a broader definition of switching).

[73] *FCC v. Midwest Video*, 440 U.S. 689, 708-09 (1979).

[74] *Id.* at 702.

[75] *Motion Pictures Ass'n of Am. v. FCC*, 309 F.3d 796, 798 (D.C. Cir. 2002) (rejecting ancillary jurisdiction to justify requiring "video descriptions" for television programming).

necessary to the furtherance of the FCC existing statutory regulatory authority over telecommunications carriers.

V. THE NPRM IS NOT IN THE PUBLIC INTEREST

Before the FCC can expand CALEA to new entities, 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."[76] The legislative history outlines three specific factors for the FCC to consider: whether it would "promote competition, encourage the development of new technologies, and protect public safety and national security."[77] In addition to the law enforcement interests cited by the NPRM, the legislative history provides broader public interest purposes for the statute as a whole, including balancing the government's interest in surveillance with the public interest "to protect privacy in the face of increasingly powerful and personally revealing technologies" and "to avoid impeding the development of new communications services and technologies."[78] The House Report reemphasizes the "national policy to promote competition in the telecommunications industry and to support the development and widespread availability of advanced technologies."[79]

The NPRM chooses to focus on the interests of law enforcement, giving short shrift to the public interest in innovation and privacy and Congress' expressed desire balance all of these interests.[80] As explained below, the expansion of CALEA to broadband Internet access and managed VOIP providers proposed in the NPRM is not in the public interest because it poses undue risks to security, innovation and privacy.

A. The NPRM Imposes Risks to Security

As the JEM Report correctly found, the additional complexity and additional points of attack that any surveillance system introduces into a communications system

---

[76] 47 U.S.C. § 1001(8)(B)(ii).

[77] House Report at 21.

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

[79] *Id.* at 14.

[80] *Compare* House Report at 13 ("the bill seeks to balance three key policies") *with* NPRM ¶ 52 (selectively quoting only the law enforcement interest portion of the legislative history's "Purpose and Scope") and ¶ 56 (calling the law enforcement interest in wiretapping an "*overriding* public interest." (emphasis added)).

create new security risks.[81] 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.

2. Vulnerabilities in operating systems or commodity software.

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.

3. Vulnerabilities in 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.[82]

---

[81] JEM Report at 47.

[82] 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. By personal

4. Vulnerabilities in 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.[83]

5. 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.[84]

---

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.

[83] 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/> (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.

[84] When a surveillance device is connected to the Internet, it may be able to leak the content 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.

6. 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.

7. 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.

8. 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 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.

B. The NPRM Poses a Risk to Innovation

The NPRM would result in all devices that provide broadband connectivity becoming CALEA-compliant, which will severely limit the scope of high-tech research and development. Today's VOIP systems would likely never have been developed in an environment where all products had to go through a CALEA-compliance test before making it to market.

With the NPRM's proposed substantial replacement test applying CALEA to Internet applications that might replace "any portion of an individual subscriber's functionality," the end result is that American innovators will always be forced to think inside the box of surveillance. Since law enforcement could argue that myriad applications replace some portion of prior functionality, the innovators' designs and ideas will be limited by a government mandate that requires them to build technology for the purpose of spying rather than playing games, talking to colleagues, or collaboratively making art over the Internet. The innovators' only other alternative would be to reverse the substantial replacement test, and ask the FCC for a decision that their specific service or application is not covered by CALEA.[85]

Since the Internet has a global reach, creativity and innovation will move off-shore, where programmers outside the U.S. can develop technologies to circumvent U.S. law enforcement capability. At the same time, U.S. companies will face competition from foreign providers who will enjoy an advantage in their time-to-market and capabilities, unbounded by the assistance capability design mandate proposed in the NPRM. For example, overseas VOIP providers could deploy surveillance-free communications software faster and with more privacy capabilities than their U.S. competitors. Thus, the rules proposed in the NPRM will stifle creativity and result in a U.S. technology marketplace that is non-competitive worldwide.

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

[85] *Compare* NPRM ¶ 61 ("providers of new services may avail themselves of existing Commission procedures to seek clarification as to whether they are covered under CALEA.") *with* 47 U.S.C. § 1001(8)(B)(ii) (requiring FCC to determine whether a particular company is a substantial replacements on a case by case basis).

problems or an inadequate response by vendors to security problems when problems are discovered.

C. The NPRM Poses a Risk to Privacy

The NPRM's harm to security and innovation will inevitably result in a risk to privacy, as products will be less secure against malicious attacks and companies will not have the market incentives to provide robust privacy protections. In addition, the NPRM will result in the following risks to privacy:

1. 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 and 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 and more carriers are asked to provide them.

There is no reason to believe that surveillance devices 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.[86] Adding surveillance capabilities to ordinary network equipment will never make the equipment more secure; but instead will likely create new vulnerabilities.

2. 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 since the original interception. 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.[87]

Deploying a surveillance device may result in recording the contents of sensitive packets which otherwise might not have been recorded, even packets whose contents were not authorized by law to be recorded and even packets sent by people who are not targets of surveillance.[88]

---

[86] *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.

[87] 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>. 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 that vary from operating system to operating system.

[88] 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.

VI. THE "TRUSTED THIRD PARTIES" MODEL IS NOT APPROPRIATE

The NPRM proposes to allow third parties to manage government surveillance requests: a private company would analyze all the data from a telecommunications carrier, extract information relevant to the court order, and send it to law enforcement.[89]

A. Abdication of Traditional Government Function

Privatizing this traditionally government function is inappropriate, and provides no assurance that private entities will safeguard the privacy and security of information not authorized to be collected.

Currently there is a vast collection of statutes, regulations and caselaw that defines the roles of law enforcement and telecommunications carriers in providing responses to law enforcement requests.[90] The NPRM proposes an alternative for which there is no legal framework for preventing the abuse of surveillance powers by private surveillance providers. For example, the ECPA defines an "electronic communications service" and a "remote computing service," and regulates these services' voluntary and required disclosure of customer communications or records.[91] Surveillance providers do not fit neatly into these definitions, and yet will have access to customer communications and records.

Intercepted customer communications can contain extremely private information, and the third-party surveillance providers approach would take this private information out of the hands of law enforcement officers (who are more likely to be concerned that the abuse of power could lead to the suppression of evidence). Private surveillance operators may be indifferent to the ultimate use of the information, and less concerned with making a clean surveillance. At the same time, private surveillance operators do not have the same incentives to protect the privacy of their customers as the information service providers proposed to be subject to CALEA.[92]

---

[89] NPRM ¶¶ 69-76.

[90] *See e.g.* Title III, ECPA and FISA, and cases interpreting these statutes.

[91] 18 U.S.C. §§ 2510(15), 2702, 2703 and 2711(2).

[92] *See e.g. Doe v. Ashcroft*, 334 F.Supp.2d 471 (S.D.N.Y. 2004) (invalidating 18 U.S.C. 2709, the "national security letter" ("NSL") provision of ECPA, on Fourth and First Amendment grounds). This case only came before the court because an ISP challenged the government's authority in order to

Currently, several large corporations already offer CALEA services that might result in a loss of privacy for consumers. For example, VeriSign offers a legal intercept service to ISPs, which requires the providers to pipe all their data to VeriSign. Then VeriSign's employees then process the court order, analyze the data, extract information relevant to the court order, and send it to law enforcement. This transaction leaves personal data potentially vulnerable when it travels from the service provider's network to VeriSign's, and places the personal data of innocent people in the hands of a third party without customer consent.

The NPRM proposal will expand this industry, putting extremely personal information in the hands of private companies without a legal framework of checks on the abuse of that power. Court ordered surveillance is, and should be, solely a government function.[93]

B. The FCC Will Create a Surveillance-Industrial Complex

The NPRM's private surveillance provider proposal will support and expand what the ACLU has called the Surveillance-Industrial Complex.[94] Since compliance with surveillance requests is a significant cost, telecommunications carriers have in the past acted as a check on government power, lobbying against excessive proposals and resisted inappropriate and overly broad requests.

Under the NPRM's proposal, however, private surveillance providers will profit from an increased amount of surveillance, and will have an incentive to lobby for more

---

protect its user's privacy. If the government has instead served the invalidated NSLs on a surveillance service provider that had a financial incentive for increased surveillance, the serious constitutional questions about NSLs may never have been raised.

[93] The NPRM's alternative proposal that the third-party surveillance companies be owned by law enforcement, *see* NPRM ¶ 75, would be constitutionally untenable, as it would provide law enforcement with unrestricted access to the raw data from the ISP, handling private information unrelated to its investigation with neither probable cause nor a court order. *See Katz v. United States*, 389 U.S. 347 (1967) (warrantless surveillance violates the Fourth Amendment), and *Berger v. New York*, 388 U.S. 41 (1967) (surveillance requires a belief that any particular offense has been or is being committed).

[94] *See* American Civil Liberties Union, *The Surveillance-Industrial Complex: How the American Government Is Conscripting Businesses and Individuals in the Construction of a Surveillance Society*, (Aug. 2004), available at <http://www.aclu.org/Files/getFile.cfm?id=16225>.

government surveillance powers and looser protections for users, further endangering privacy.

VII. CONCLUSION

The rules proposed by the NPRM 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."[95] Ultimately, the problems noted above can be traced back to a single root cause: CALEA was drafted specifically to regulate phone networks, which are designed to be closed systems. The Internet is an open, global system that handles countless forms of data-transfer and accommodates an ever-changing array of hardware and software devices. If CALEA is misapplied to the Internet, the results will be disastrous. The privacy of innocent people is likely to be violated, innovation will certainly be stifled, and the current and future functionality of the Internet will be crippled.

A. Drop the NPRM Altogether

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 Voice Over IP providers, are not subject to CALEA.

B. Alternative: Establishing a CALEA Task Force

If the FCC still wishes to consider expanding CALEA, 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 the anecdotal evidence presented so far.

The EFF suggests that the FCC 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,

[95] 47 U.S.C. § 230(b).

computer security experts, and the consumer electronics industry to examine at least the following questions:

1. How well has CALEA worked so far?
2. Has CALEA been abused?
3. How much has CALEA cost society, and how much will its expansion cost?
4. How will CALEA affect national innovation and global competitiveness?
5. How will CALEA's expansion to the Internet affect the privacy and security of private communications?

Respectfully submitted,

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

November 8, 2004