Communications Assistance for Law Enforcement Act (CALEA)

Lieutenant Commander Andrew Henderson[*]

In investigating terrorism, espionage, and other serious crimes, electronic surveillance is not only one of the most effective tools government has, but often the only effective tool.[1]

Introduction

The rapidly changing landscape of telecommunication technologies and the introduction of digitally-based services and features have impeded law enforcement's ability to consistently effectuate court-authorized electronic surveillance.[2] This impedance hinders law enforcement's ability to protect communities nationwide from the harms inflicted by organized crime and terrorism.[3] In response to this threat and in the interests of public safety and national security,[4] the Federal Communications Commission (FCC) recently adopted a rule "establishing that providers of facilities-based Internet access services and providers of interconnected voice over Internet Protocol (VoIP)[5] services . . . must comply with the Communications Assistance for Law Enforcement Act (CALEA)."[6]

As Senator John McCain noted, "[s]ince [VoIP] is a breakthrough technology, there's going to be a lot of china broken [in crafting legislation]."[7] It is therefore perhaps not surprising that not everyone is happy with the FCC ruling. Industry, for example, has contested both the authority of the FCC "to extend CALEA to the broadband Internet"[8] and the imposition of government control over the design of software applications and electronic devices.[9] Colleges and universities fear the high costs the ruling will levy on them as service providers.[10] The American Civil Liberties Union (ACLU) has voiced concerns over the ruling's effects on personal privacy.[11] A review of both the law and the policy behind the FCC ruling, however, shows the decision to be legally sound, procedurally valid, and grounded in sound policy designed to lawfully protect national security.

---

[*] Judge Advocate General's Corps, U.S. Navy. Presently assigned as Commander, Deputy Force Judge Advocate for Commander, Naval Air Forces in San Diego, California. J.D. 1993, Pepperdine University School of Law; M.A. 2004, University of Redlands School of Business; B.A. 1989, Bates College.

[1] *Law Enforcement Access to Digital Communication: Hearing Before the Subcomm. on Telecomm. and the Internet of the H. Comm. on Energy and Commerce*, 108th Cong. (2004) [hereinafter Parsky Statement (House)] (statement of Laura H. Parsky, Deputy Ass't Att'y Gen. Crim. Div., U.S. Dep't of Just.).

[2] *See* Implementation of Section 109 of the Communications Assistance for Law Enforcement Act, 62 Fed. Reg. 13,307 (Mar. 20, 1997) (codified at 28 C.F.R. pt. 100 (2006)).

[3] *See The VOIP Regulatory Freedom Act of 2004: Hearing on S. 2281Before the S. Comm. on Commerce, Science, and Transportation*, 108th Cong. (June 16, 2004) [hereinafter Parsky Statement (Senate)] (statement of Laura H. Parsky, Deputy Ass't Att'y Gen. Crim. Div., U.S. Dep't of Just.).

[4] *See* Communications Assistance for Law Enforcement Act and Broadband Access and Services, 70 Fed. Reg. 59,664, 59,667 (Oct. 13, 2005) (to be codified at 47 C.F.R. pt. 64) [hereinafter FCC Ruling].

[5] Voice Over Internet Protocol (VoIP), also known as IP or Internet telephony, converts voice to data that is routed through the Internet, like e-mail, via broadband networks. *See* What's VoIP?, http://www.vonage.com/help_vonage.php (last visited Mar. 28, 2006).

[6] FCC Ruling, *supra* note 4, at 59,664.

[7] *The VOIP Regulatory Freedom Act of 2004: Hearing on S. 2281 Before the S. Comm. on Commerce, Science, and Transportation.*, 108th Cong. (2004) (statement of Sen. John McCain, Chairman, S. Comm. on Commerce, Science and Transportation).

[8] *Id.* (statement of James X. Dempsey, Exec. Dir., Ctr. For Democracy and Technology) [hereinafter Dempsey Statement (Senate)].

[9] *See* Marcia Coyle, *Tapping the Net; FCC Ruling That Broadband Services Accommodate Wiretaps in Their Designs Likely To Go To Court*, MIAMI DAILY BUS. REV., Aug. 18, 2005, at 9.

[10] *See* Sam Dillon & Stephen Labaton, *Colleges Oppose Call to Upgrade Online Systems*, N.Y. TIMES, Oct. 23, 2005, at A1.

[11] *See* Coyle, *supra* note 9, at 9.

CALEA

The legal structure for electronic surveillance originated with the seminal Supreme Court case of *United States v. Katz*.[12] In *Katz*, the Court held for the first time that government interceptions of telephone conversations are regulated by the Fourth Amendment.[13] In the wake of *Katz*, Congress set rules for intercepting telephone calls through the Omnibus Crime Control and Safe Streets Act of 1968, Title III.[14] In 1970, Congress clarified the law, directing that a court order "should, at the request of the officer applying for authority, direct the provider to furnish the applicant with the necessary 'information, facilities and technical assistance.'"[15]

In 1994, Congress enacted CALEA[16] to address the rapidly changing face of telecommunication technology and to "extend and clarify the previous obligations of telecommunications service providers to assist law enforcement with electronic surveillance orders."[17] To effectuate this intent, CALEA requires telecommunications carriers "to ensure that their equipment, facilities, and services adhere to standards that enable law enforcement to pursue call intercepts, pen registers, and trap and trace technologies for surveillance."[18]

Federal Communications Commission Implementation

The CALEA gives the FCC broad discretion in defining which persons or entities are governed by the statute. Specifically, the FCC may find a provider (person or entity) to be a "telecommunications carrier" when its provision of "wire or electronic communication switching or transmission service . . . is a replacement for a substantial portion of the local telephone exchange service and that it is in the public interest to deem such a person or entity to be a telecommunications carrier. . . . "[19] Specifically exempted, however, are persons or entities engaged in "information services," which the statute defines as "generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications."[20]

Utilizing the authority vested by CALEA, the FCC recently determined that the statute applied to some non-traditional telecommunications service providers: Broadband Internet Access Services and VoIP Services.[21] In both cases, the FCC applied a three-prong test. First, the FCC found that both service providers provided a switching or transmission functionality.[22] Second, it determined the providers replaced a substantial portion of the local telephone exchange service.[23] Third, the FCC specifically found a public interest in favor of such a determination, weighing "the effect on competition, the development and provision of new technologies and services, and public safety and national security."[24]

---

[12] 389 U.S. 347 (1967).

[13] *See* CALEA Implementation Section – Federal Bureau of Investigation, *Communications Assistance for Law Enforcement Act (CALEA)*, http://www.doj.gov/criminal/cybercrime/usamay2001_4.htm (last visited Mar. 20, 2006).

[14] Omnibus Crime Control and Safe Street Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (codified as amended at 18 U.S.C.S. §§ 2510-22 (LEXIS 2006).

[15] *See* 18 U.S.C.S. § 2518 (LEXIS 2005).

[16] 47 U.S.C.S. §§ 1001-1021.

[17] Christopher Guttman-McCabe et al., *Homeland Security and Wireless Telecommunications: The Continuing Evolution of Regulation*, 57 FED. COMM. L. J. 413 (2005).

[18] *Id.*

[19] 47 U.S.C.S. § 1001.

[20] *Id.*

[21] *See* Communications Assistance for Law Enforcement Act and Broadband Access and Services, 70 Fed. Reg. 59,664, 59,667-68 (Oct. 13, 2005) (to be codified at 47 C.F.R. pt. 64).

[22] *See id.* at 59,666—59,668.

[23] *See id*.

[24] *See id.*

The FCC also specifically found that the CALEA Information Services Exclusion[25] did not apply to either type of provider. In its determination, the FCC found that while many providers offer both telecommunications and information services, CALEA did not require the classification of an integrated service offering as solely one or the other.[26] The additional provision of information services, in other words, does not preclude the application of CALEA to a provider of telecommunications services.

Public Concerns

Federal Communication Commission Authority

The focus of industry arguments against the FCC's authority to bring Broadband and VoIP providers under CALEA revolve around interpretations of legislative intent gleaned from congressional committee reports from the early 1990s. Thus the Internet, some industry leaders argue, was clearly seen as an information service to be excluded by CALEA.[27] "The FCC," said one legal analyst, "is legislating, not interpreting."[28]

This rationale fails for two reasons. First, from a practical standpoint, though experiments began as early as 1974, commercially viable VoIP did not exist when CALEA was drafted.[29] Congress, however, drafted CALEA with foresight, and the statute "requires that, as new technologies are developed, providers act responsibly by engineering their systems in a way that allows law enforcement to execute court-ordered electronic surveillance."[30]

Second, Congress expressly provided the FCC with the authority to find that providers of wire or electronic switching could ultimately become telecommunications carriers in the event that they replaced substantial portions of the local telephone exchange service. Critics do not appear to have attacked either of the first two prongs utilized in the FCC decision, namely that these services provide switching/transmission features and that they replace substantial portions of the local telephone service. Their focus instead is a narrowly tailored attack on the public policy prong—specifically, government involvement in design and cost allocations.

Government Involvement in Design

The industry concern is that the requirement to produce a "surveillance-ready cell phone"[31] and other such equipment is, in effect, the intrusion of law enforcement into the "design of applications and devices."[32] Such government involvement is contrary to public policy, it is reasoned, because "[t]he tremendous economic growth that has accompanied the Internet's rise would not have happened if everything had been forced to get approval of a government agency."[33] Or as Christopher Calabrese of the ACLU's Technology and Liberty Project laments, "it could give the FBI a sort of check on the expansion of communications technology in the U.S. if they can pre-vet and say you have to be CALEA-compliant. . . ."[34]

---

[25] 47 U.S.C.S. § 1002(b)(2). The Communications Assistance for Law Enforcement Act specifically waives compliance requirements for information services or "equipment, facilities, or services that support the transport or switching of communications for private networks or for the sole purpose of interconnecting telecommunications carriers." *Id.*

[26] *See id.* at 59,666.

[27] *See* Dempsey Statement (Senate), *supra* note 8.

[28] Coyle, *supra* note 9 (quoting Susan Crawford, "cyber law scholar," Yesheva University's Benjamin N. Cardozo School of Law).

[29] *See* E-mail from Jeff Pulver, Vonage Founder, to Andrew H. Henderson (author) (Mar. 29, 2006) (on file with author).

[30] Parsky Statement (House), *supra* note 1.

[31] Coyle, *supra* note 9, at 9.

[32] *Id.*

[33] *Id.* (quoting Susan Crawford, "cyber law scholar," Yesheva University's Benjamin N. Cardozo School of Law).

[34] *Id.*

The CALEA, however, makes no claim on design specifics—but rather on end-state performance. And there are no statutory requirements that new technology be vetted through federal law enforcement prior to production. On the contrary, law enforcement is barred from dictating design specifics, as CALEA "'does not authorize any law enforcement agency or officer . . . to require any specific design. . . to be adopted by any provider [or] manufacturer, . . .' and it does not authorize any law enforcement agency or officer 'to prohibit the adoption of any equipment, facility, service, or feature by any provider . . . [or] manufacturer.'"[35]

Further, CALEA has been around since 1994—it is only the application of CALEA to Broadband and VoIP providers that is recent. The worst-case scenario painted by its critics makes no showing of how the telecommunications industry has been technologically stymied by the FBI over the last eleven years. One might argue it has instead thrived.

Costs of Implementation

Another great concern about the application of CALEA to Broadband and VoIP providers is cost. Universities alone claim it would cost them $7 billion to become CALEA-compliant under the new FCC policy, deeming it "the mother of all unfunded mandates."[36] The formula for the derivation of this figure is unclear, but it rings somewhat far-fetched. In the first place, government officials do not expect costs to be particularly high for universities because the FCC order "did not require surveillance of networks that permit students and faculty to communicate only among themselves, like intranet services."[37]

In addition, the FCC is considering whether to exempt educational institutions from some of the law's provisions;[38] however, it seems unlikely the $7 billion worst-case scenario has factored in CALEA's protective provisions. First of all, CALEA "allows carriers to seek a determination of whether implementation of a CALEA solution is 'reasonably achievable' in light of costs and other issues."[39] It does not, therefore, allow law enforcement to place a blanket demand on carriers to meet some arbitrary gold standard. Secondly, while CALEA expects industry to bear the cost of ensuring that new equipment meets the legislated requirements, the statute "provides that the Federal government will pay carriers for just and reasonable costs incurred in modifying existing equipment, services or features to comply with the capability requirements . . . [and for] expansions in capacity to accommodate law enforcement needs."[40] As many carriers have been reimbursed by the federal government for various CALEA costs to date,[41] panic appears at best premature.

Privacy

Finally, there is the argument that CALEA erodes constitutional protections and threatens individual privacy rights. But "nothing in CALEA gives law enforcement the authority to conduct any surveillance. [It] is about the practical necessity of implementing existing lawful authority, not expanding authority."[42] On the contrary, the statute protects privacy. First, it protects the privacy of other system users by requiring that service providers be able to readily separate the communications of a particular subscriber whose communications law enforcement has a court order to intercept.[43] Second, "CALEA requires that a service provider be able to separate call-identifying information from the content of communications. This protects the call content from law enforcement access where law enforcement only had legal grounds to obtain the call-identifying

---

[35] Parsky Statement (House), *supra* note 1 (quoting CALEA Section 103, 47 U.S.C. § 1002(b)(1) (LEXIS 2006)).

[36] Dillon & Labaton, *supra* note 10, at A1 (quoting Terry W. Hartle, Senior Vice President, American Council on Education).

[37] *Id.*

[38] *See id.*

[39] Parsky Statement (House), *supra* note 1.

[40] H.R. REP. NO. 103-827, pt. 1 (1994).

[41] *See* Ted Hearn, *Taming Cyberterrorists Via Broadband; FCC Puts Internet-based Services Into The CALEA Camp*, MULTICHANNEL NEWS, Aug. 16, 1994, at 20.

[42] Parsky Statement (Senate), *supra* note 3.

[43] *See* Parsky Statement (House), *supra* note 1.

information."[44] This allows law enforcement to pinpoint its searches and prevents unnecessary "rummaging" through protected communications.

CALEA Applicability

Department of Defense

The federal government, and particularly the Department of Defense (DOD), owns an expansive broadband computer network. Do the new CALEA regulations apply to its systems? According to cyber attorney Fran Walterhouse, Principal Legal Advisor for Computer Crime at the U.S. Army Criminal Investigation Command, the present DOD stance is that "communications carrier" refers to "a common carrier for hire or otherwise on a commercial basis available to the public."[45] While this interpretation seems to make sense, it is not specifically expressed as such in the statute. Further, if in fact university systems are ultimately determined to fall within the purview of CALEA, might not DOD systems, too, be regulated? Given the newness of the FCC ruling, this issue has yet to be broached officially.

European Economic Union

Lastly, it is important to remember that in our global economy, the hardware, software, and even actual service providers may not originate on U.S. soil. With no European "FCC" to take the lead overseas,[46] the extent to which CALEA may be applied extraterritorially is unclear. Thus, while the United States may be able to ban the import of phones, switches, or routers that are not CALEA-compliant, it may be considerably more difficult to enact a search warrant, for example, on a call placed through a foreign-based VoIP or Broadband provider.

Conclusions

The recent FCC ruling on CALEA was specifically premised on the "protection of public safety and national security."[47] The CALEA is over a decade old and has helped law enforcement arrest over 54,000 suspects since it was enacted.[48] It is a vital component in the war on terror, as "the cell structure and worldwide scope of modern terrorist groups make electronic surveillance essential to uncovering these lethal networks before they strike us in ever more devastating ways."[49] It does not afford law enforcement any additional search authority and merely expands existing statutory requirements to advancing technology. While there may be some legitimate concerns regarding cost of implementation, there are protective measures in the statute to ensure carriers do not bear a disproportionate burden. Although cost is not irrelevant, on balance with the global dangers the United States faces today, it seems the least of our worries.

---

[44] *Id.*

[45] E-mail from Fran Walterhouse, Principal Legal Advisor for Computer Crime, U.S. Army Criminal Investigation Command, to Andrew H. Henderson (author) (Nov. 9, 2005) (on file with author).

[46] *See* Axel Spies, *Telecom In Europe: Disharmonies In The Regulatory Concert—Swindler Berlin LLP*, MONDAQ BUS. BRIEFING, Oct. 24, 2005.

[47] Communications Assistance for Law Enforcement Act and Broadband Access and Services, 70 Fed. Reg. 59,664, 59,664 (Oct. 13, 2005) (to be codified at 47 C.F.R. pt. 64).

[48] *See* Parsky Statement (House), *supra* note 1.

[49] *Id.*