

NATOA[®]

JOURNAL OF
Municipal
Telecommunications
Policy

Legislative Review and Forecast for 2005



CALEA and law enforcement surveillance in the era of homeland security:

What Does the IP-Enabled Future Hold?

For good reason, much has been written about the dangers facing local franchising authorities in connection with the migration of communications to “packet mode” platforms and technologies. But cable regulators are not the only local officials whose lives are being made more difficult by this trend. Beyond the now-familiar threat that video programming may soon be provided via Internet Protocol (thereby threading the regulatory needle in a manner that may evade local authority), the job of local law enforcement is being made significantly more complicated by the packet mode revolution.

Legislative Review and



Forecast for 2005

BY WILLIAM R. HANNA

Law Enforcement Surveillance

Voice over Internet Protocol (VoIP) telephone service is perhaps the best-known example of the rise of packet-mode technologies, which transport voice, video and data as “packets” of digital data that may be separated and rearranged in transmission and subsequently reassembled for delivery at their destination. VoIP has been around for years, but until recently was plagued by voice-quality and latency (delay) problems that prevented its widespread adoption. Now that technology has largely solved such problems, the quality of VoIP calls rivals that of plain old fashioned telephone service (POTS) calls placed over the public switched telephone network. With quality improved, VoIP use has grown rapidly, perhaps due to perceived consumer value (VoIP providers generally offer unlimited local and long-distance calls for a fixed monthly fee and many offer advanced calling features not available from traditional telephone companies). There is abundant evidence that VoIP and other packet-mode technologies are quickly supplementing, and may eventually replace, traditional technologies like POTS.

The problem is that as even more communication moves to new platforms, less and less of it is easily monitored by law enforcement — a potentially disastrous trend in this post September 11th world. It’s a little ironic that even as recognition grows of the importance of local police and Sheriffs’ departments as Homeland Security first responders, the very ability of local law enforcement to fulfill that role by conducting critical electronic surveillance is compromised by the movement of communications to non-traditional platforms. Moreover, due to the hands-off approach advanced by the Federal Communications Commission (FCC) with respect to new communications technologies generally, even the laws specifically designed to ensure that law enforcement surveillance techniques keep pace with technology have failed.

A case in point is the Communications Assistance for Law Enforcement Act (CALEA), enacted in 1994 in order to preserve law enforcement’s ability to conduct electronic surveillance *despite changes* in technology. 2004 saw several developments that affected law enforcement’s ability to stay abreast of the paradigm shift underway in telecommunications including, specifically, how CALEA is to be interpreted and applied with respect to the new technologies. In December 2003, the FCC formed an Internet Policy Working Group to help identify, evaluate and address policy issues associated with the movement of telecommunications to Internet-based platforms. Then, in February 2004, the FCC issued its IP-Enabled Services NPRM.¹ The FCC had previously determined that one type of VoIP service is an “information service” free

from state or local regulation.² In the IP-Enabled Services NPRM, the Commission asks whether all such services should be treated similarly.

FCC determinations regarding the classification and regulation of packet mode technologies will significantly affect the ability of all law enforcement agencies — federal, state and local — to conduct lawful electronic surveillance because depending on how such technologies are classified, CALEA may or may not apply. If CALEA ultimately is held not to apply to new developments in telecommunications, it is inconceivable that law enforcement will be able to keep pace with the rapid changes in communications technology.

By way of background, Congress passed the Omnibus Crime Control and Safe Streets Act (OCCSSA) in 1968 to establish the procedures that govern electronic surveillance performed by law enforcement.³ Two years later, Congress established that it was the duty of communications service providers to provide technical assistance to law enforcement in order to enable lawful electronic surveillance intercepts.⁴ Technology marched on, of course. And so in 1986, Congress was compelled to pass the Electronic Communications Privacy Act (ECPA)⁵ to clarify that the OCCSSA covered then-nascent electronic communications tools such as cellular telephones, pagers, facsimiles and e-mail.

Fast forward to 1994. Cell phones and facsimiles were old news by this time. Recognizing that technology and the telecommunications industry would continue to evolve, Congress enacted CALEA to preserve law enforcement’s ability to conduct lawful electronic surveillance. CALEA provided law enforcement with no new or expanded surveillance authority. Instead, it sought to ensure that the purposes of the OCCSSA and the ECPA were accomplished by better defining the obligations of telecommunications providers to provide electronic surveillance capabilities and by requiring industry to develop and deploy CALEA intercept solutions for the problems posed by new technologies.

According to law enforcement authorities, by the time the FCC commenced its IP-Enabled Services NPRM in February 2004, it was clear that CALEA’s purpose had been frustrated. On March 10, 2004, the United States Department of Justice, the Drug Enforcement Administration and the Federal Bureau of Investigation jointly petitioned the FCC for an expedited rulemaking concerning CALEA’s application to new communications technologies.⁶ The primary issue identified in the joint petition is the fact that CALEA applies only to “telecommunications carriers,” as it defines them. Although CALEA defines “telecommunications carrier” more broadly than the

¹ In the Matter of IP-Enabled Services, WC Docket No. 04-36, Notice of Proposed Rulemaking, FCC 04-28 (rel. Mar. 10, 2004).

² Petition for Declaratory Ruling that pulver.com’s Free World Dialup is Neither Telecommunications Nor a Telecommunications Service, WC Docket No. 03-45, Memorandum Opinion and Order, FCC 04-27 (rel. Feb. 19, 2004).

³ Omnibus Crime Control and Safe Streets Act, Pub. L. No. 90-351, 82 Stat. 212 (1968) (OCCSSA).

⁴ Pub. L. No. 91-644, 84 Stat. 1880 (1970), amending Title III of the OCCSSA.

⁵ Pub. L. No. 99-508, 100 Stat. 1848 (1986).

⁶ In the Matter of United States Department of Justice, Federal Bureau of Investigation and Drug Enforcement Administration, Joint Petition for Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance for Law Enforcement Act, RM 10865 (filed March 10, 2004).

According to law enforcement authorities, by the time the FCC commenced its IP-Enabled Services NPRM in February 2004, it was clear that CALEA's purpose had been frustrated.

Communications Act, the FCC's decisions concerning new technologies had created a situation in which CALEA's scope was unclear. The joint petition noted that, "many entities ... claim that they and/or their services are not CALEA-covered, and ... roll out new services with minimal, if any, interception capabilities." As a result, the Joint Petition stated, "[t]he ability of federal, state, and local law enforcement to carry out critical electronic surveillance *is being compromised* today by providers who have failed to implement CALEA-compliant intercept capabilities. Communications among surveillance targets are being lost, and associated call-identifying information is not being [timely] provided...."

The joint petition asked the Commission, among other things, to:

- Identify the types of services and entities that are subject to CALEA;
- Identify which services are considered "packet-mode services;"
- Declare that broadband access and broadband telephony services are subject to CALEA; and
- Adopt rules for identifying new CALEA-covered services and providers.

The requested relief, according to the joint petition, would put "both law enforcement and industry...on notice with respect to CALEA obligations and compliance." Because the FCC had already espoused a light regulatory touch with respect to VoIP, the joint petition concentrated on the different definitions of "telecommunications" used in CALEA and the Communications Act, arguing that distinctions between them would permit the Commission to declare that IP-enabled services are subject to CALEA — without necessarily finding that they are subject to common-

carriage rules under the Communications Act.

In response to the joint petition, the FCC on August 9, 2004 released a new NPRM and Declaratory Ruling in which it "tentatively concludes," among other things, that: (1) CALEA's definition of "telecommunications carrier" was intended by Congress to be broader than the definition in the Communications Act; and (2) facilities-based providers of broadband Internet access service are indeed subject to CALEA.⁷ But in the CALEA NRPM, the Commission stresses "that [these] tentative conclusions ... in no way predispose how the Commission may proceed with respect to adopting a regulatory framework for [IP-enabled] and broadband services or determining their legal classification under the Communications Act."⁸

For better or for worse, some uncertainty about the direction the FCC will take regarding regulation of packet-mode services may have been removed with President Bush's recent reelection. But like so many issues in the "packet mode" world, it appears that final resolution of the issues raised in the joint petition and addressed in preliminary fashion in the CALEA NPRM is still to come. Congress has acted a number of times to ensure that law enforcement have the ability to continue to engage in lawful electronic surveillance, even as new communications technologies and services are developed, and the FCC would do well to honor Congress's intent in this respect. Should the FCC fail to give serious consideration to their needs, municipal and other law enforcement authorities may soon face serious challenges to the proper performance of their duties, even as public recognition of the importance of those duties grows. For municipal law enforcement officials tasked with front line Homeland Security and "first responder" responsibilities, the debate is vitally important. ■

⁷ In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services, ET Docket No. 04-295, RM-10865, Notice of Proposed Rulemaking, FCC 04-187 (rel. Aug. 9, 2004), at ¶1.

⁸ Id. at fn 1.