

CALEA: Prepare for the Worst, Hope for the Best

On August 5, 2005, nearly a year since requesting public comment on the issue, the Federal Communications Commission (FCC) voted to extend the Communications Assistance for Law Enforcement Act (CALEA) to broadband Internet and interconnected Voice-over-Internet Protocol (VoIP) providers. This includes college and university campus networks, as well as state and regional educational networks. The order requires that providers come into compliance by late spring of 2007. At this time, the exact requirements for compliance are not known, but many speculate that the worst-case scenario would involve replacing a significant fraction of switches and routers that are capable of connecting to the public Internet or the public switched telephone network (PSTN).

Background

To understand CALEA, one needs to understand wiretapping, or the use of “legal intercepts.” Wiretapping is one of many tools that law enforcement uses to gather evidence. Since 1968, there have been strict procedures that law enforcement must follow in order to conduct a legal intercept, and CALEA does not change that. But in the 1980s, after the breakup of AT&T—when many new phone providers entered the market, cell phones became popular, and there was a major shift from analog to digital signals—wiretapping became increasingly more difficult and expensive to execute. In the early 1990s, law enforcement asked Congress for assistance.

CALEA was originally passed by Con-

gress in 1994 “to make clear a telecommunications carrier’s duty to cooperate in the interception of communications for law enforcement purposes.”¹ The act requires providers of commercial voice services to engineer their networks and their operations to assist in executing wiretap orders. At the time, and only after months of hearings and negotiations, the Internet and private phone networks were exempted from the requirements as part of a compromise.

Ten years later, in the spring of 2004, law enforcement was again feeling disadvantaged due to the pressure of advancing technology. Communications for the general public and criminals alike were migrating from the telephone system (covered under CALEA) to the broadband Internet (not covered under CALEA). VoIP was available to the public, and increasingly, people were getting their Internet connections from broadband rather than dial-up. The Department of Justice, the FBI, and the Drug Enforcement Agency jointly petitioned the FCC to reinterpret CALEA to include not just commercial voice service providers but any facilities-based Internet service provider (ISP).

In a series of documents and discussions from April 2004 through August 2005, law enforcement proved, to the satisfaction of the FCC commissioners, that broadband had become a substantial replacement for dial-up Internet access (thereby replacing local telephone exchange services) and that VoIP had become a substantial replacement for telephone service. The argument was based on a CALEA provision called the Substantial Replacement Provision. This

provision states that the term “telecommunications carrier” can include any “person or entity engaged in providing wire or electronic communication switching or transmission service to the extent that the Commission finds that such service is a replacement for a substantial portion of the local telephone exchange service.”² This line of reasoning was buoyed by the widely accepted claim that criminal behavior had migrated to the Internet and that, in fact, the Internet had become the communications “vehicle of choice” for criminal activity, including terrorism. CALEA had become an issue of national security.

The Higher Education Community Responds

In April 2004 and again in November 2004, EDUCAUSE formed a coalition of fifteen education and library associations and responded to the FCC request for comments on the petition by law enforcement, as well as the subsequent Notice of Public Rulemaking. The associations’ comments outlined two main arguments. The first was a legal one: extending CALEA to facilities-based Internet providers would require a rewrite of the original act, and thus Congress, not the FCC, should make that decision. Transcripts from the original hearings were used to illustrate that Congress clearly had not intended for CALEA to extend to the Internet. This argument was rejected in the FCC First Report and Order, passed on August 5, 2005.

However, also stated in the associations’ comments was a second argument, one based on the public interest. This argument reasoned that even if the act is

extended to cover facilities-based ISPs, it is in the public interest to exempt education and library networks. This rationale used a cost/benefit analysis to show that for the few wiretaps executed annually on campuses or in libraries, the cost of compliance had no justification. In addition, this argument stated that sufficient information could be obtained without compliance and that compliance would have a detrimental effect on innovation. This issue has not been decided: the FCC issued a Further Notice of Proposed Rulemaking to gather additional information on possible exclusions from full compliance for, among others, education and research networks. EDUCAUSE joined the American Council on Education (ACE) and other higher education groups to once again file comments, on November 14, 2005.³ The FCC promised a Second Report and Order that will address these issues.

In light of the present circumstances (a First Report and Order stating that higher education must be compliant by late spring 2007 and a pending Second Report and Order covering any special considerations), the higher education community has decided to move forward using a multipronged approach:

- The higher education community will try to get the First Report and Order overturned and the issue sent to Congress. To accomplish this, ACE, on behalf of higher education, filed a Petition for Review⁴ with the U.S. Court of Appeals for the District of Columbia on October 24, 2005. (The library community has joined with several other public interest and industry groups to file a similar petition.⁵)
- The higher education community will try to secure an FCC rule excluding the higher education community from at least some of the more burdensome compliance requirements. To accomplish this, the higher education community, through the leadership of ACE, has filed comments in the latest FCC rulemaking procedure.
- The higher education community will try to negotiate a compromise with the Department of Justice. To accomplish this, the higher education community, through ACE and EDU-

CAUSE, will continue the negotiations, started a year ago, to try and arrive at an agreement that will assure law enforcement of continued and improved cooperation by campus and network personnel but that will avoid the tremendous expense anticipated for full compliance by higher education.



Looking Ahead

As of this writing, there are numerous unanswered questions about the potential impact of CALEA on college, university, state, and regional educational networks. Little was clarified by the August 5 First Report and Order except that these networks are covered and will need to be fully compliant by the spring of 2007. Of course, foremost in everyone's mind is the question of cost.

Cost is literally the "million-dollar" question. Currently, the worst-case scenario requires the replacement of a significant portion of the switches and routers in a network. Based on the size of the campus network and the replacement cycle of current network equipment, this cost could be substantial. One large campus recently spent nearly \$18 million to upgrade its routers and switches. Of course, this cost could vary dramatically depending on what the final standards of compliance are and what type of agreement is reached with the Department of Justice.

What do we know about compliance requirements? Capability requirements,⁶ as spelled out in the original CALEA, are available, and the FCC

promises more specific information in the Second Report and Order. In addition, the Telecommunications Industry of America (TIA) has a set of standards available for Lawfully Authorized Electronic Surveillance (J-STD-025-B).⁷ However, these standards have been rejected by law enforcement as inadequate. The clear definition of CALEA compliance for facilities-based ISPs should become more apparent in the coming months. Along with the FCC Second Report and Order, law enforcement is working on a standards document that builds on the TIA standard.

Another source for information is the equipment suppliers. Vendors currently provide CALEA-compliant equipment for commercial ISPs but apparently have not extended their line of compliant equipment into the market that would include college and university campus networks. Developments in this area are sure to take place when the court makes a decision as to the legality of the First Report and Order and when the level of demand becomes more apparent.

Few analysts predicted that the First Report and Order would be voted on and passed in August 2005; the months ahead are no less uncertain. For now, the next steps for the higher education community depend on the interaction between five major players: Congress, the court system, the Department of Justice, the FCC, and ACE. "Prepare for the worst, hope for the best" seems to be appropriate advice.

Notes

1. Communications Assistance for Law Enforcement Act of 1994, HR 4922, 103d Cong., 2d sess. See <<http://www.askcalea.net/calea.html>> for the full text of the act.
2. CALEA, §102(8)(B)(ii).
3. Comments submitted by the "Higher Education Coalition" to the FCC on CALEA on November 14, 2005, <<http://www.educause.edu/ir/library/pdf/EPO0536.pdf>>.
4. The Petition for Review is available at <<http://www.educause.edu/ir/library/pdf/CSD4263.pdf>>.
5. See the American Library Association Web site for details: <<http://www.ala.org/ala/washofi/WOissues/techinttele/calea/calea.htm>>.
6. For the CALEA capability requirements, see <<http://www.educause.edu/ir/library/pdf/CSD4234.pdf>>.
7. TIA's standards are available at <http://www.tiaonline.org/standards/search_results2.cfm?document_no=J-STD-025>.

Wendy Wigen is a policy analyst with EDUCAUSE.