



Policy Briefing: CALEA compliance for educational organizations

CALEA compliance as an emerging issue for educational network operators

The Communications Assistance for Law Enforcement Act (CALEA) defines the legal obligations communications providers have to assist law enforcement agencies in setting up court-ordered wiretaps. CALEA does not govern when a wiretap can be ordered—that is controlled by other laws—but sets guidelines about who must do what in response to a court’s wiretap order. Historically, CALEA has been applied primarily to telephone companies. New rulings by the Federal Communications Commission (FCC) extend the provisions of CALEA to providers of broadband Internet access and interconnected voice-over-IP services. Although further clarification is needed, this change suggests that the obligations of CALEA compliance are extended to any organization that provides broadband Internet access or VoIP services.

CALEA and educational organizations

Under the FCC’s broadened definitions, CALEA arguably now applies to all network operators, including educational institutions and libraries, with a compliance deadline of May 14, 2007. This implies that such organizations would have new obligations to prepare their networks to provide access to law enforcement wiretaps in response to a court order. The technical details of providing such access are not entirely resolved as they apply to packet-based services like Internet communication and VoIP. However, there is an implication that a network operator would either need to install network hardware or software that would facilitate wiretapping, or engage a trusted third party to perform the wiretapping function on its behalf. Organizations bound by CALEA must document their readiness to comply with wiretapping orders and must have response procedures in place. The costs of compliance are not covered by the FCC or law enforcement.

Possibilities for exemption from CALEA

The FCC order and relevant court papers have lead to a prevailing interpretation that an educational institution should be fully exempt from CALEA if it satisfies two criteria: 1) it does not “support” the connection of the private network to the Internet and 2) its network qualifies as a “private network.” These terms are not fully defined within the Act, but suggest a means for avoiding the cost and obligations of CALEA compliance.

Defining “supporting” the connection to the Internet

In court proceedings, the FCC stated that it did not intend to impose CALEA obligations on organizations that contract with a network provider for their connection to the Internet. Rather, CALEA would apply to organizations that use their own circuitry and hardware to connect to a major Internet exchange point. This indicates that probably most organizations satisfy this portion of the exemption, since typically only service providers and very large organizations connect directly to the top-tier Internet exchange points.

Defining a “private network”

Neither the CALEA statute nor the FCC’s rules clearly define the term “private network.” Certainly to be included are those networks—rare today—that do not interconnect with any other network or the Internet. Further, though, the FCC’s order implies that interconnected networks can still qualify as private when they are accessible only by an organization’s constituents—such as students, faculty and staff in the case of an educational institution. Some degree of guest or transient access may also be acceptable, but limits on such access have not been defined or tested in court. There is currently disagreement on this point among legal analysts; the aspect of providing “members-only” access may prove to be entirely irrelevant, leaving the issues of “supporting the connection to the Internet” as the key factor.

Taken together, these two criteria may prove to exempt a very large portion of education and research organizations. Gray areas remain, though, for organizations that allow some degree of unauthenticated public access to their networks (say, via public wireless LANs), or that have particular network configurations that are not fully reliant on Internet service providers. Ultimately, each institution’s legal counsel will provide specific guidance on compliance requirements.

This briefing is for the general information of the Merit community. You should consult legal counsel for advice on the specific needs and requirements of your organization.

CALEA compliance for non-exempt network operators

Given the limitations implicit in meeting the two exemption criteria, some organizations may wish to consider coming into compliance with CALEA and preparing to provide wiretap access. This would require establishing a formal set of procedures to be followed upon receiving a court order, building the technical capability to conduct wiretaps either directly or through a trusted third party, and filing compliance reports with the FCC. Specifics for each of these steps is not yet clear and best-practice advice will emerge in the coming months. It should be noted that CALEA does not add to or subtract from existing legal authority for courts to subpoena information and request wiretaps. These laws are independent of CALEA and will continue to be applied as they have been. **It is important for any organization to establish clear policies and procedures for handling court orders to surrender information or provide surveillance assistance.**

The development of technical specifications for compliance

The technical specifics of complying with CALEA are not established by the Act. Rather, CALEA broadly defines requirements and leaves specific implementations to industry to develop. Technologies and approaches for broadband Internet and VoIP providers are being discussed by industry groups and corporations. It is important to understand that there is not a “CALEA protocol” that organizations will be expected to build their networks around. Rather, network operators are free to present any plan that reasonably accommodates the Act. It is expected that many approaches will emerge from industry and general practice.

Next steps with CALEA

Any organization that operates a broadband Internet network or provides Voice over IP services must consider its potential obligations under CALEA. For most organizations, this will require an analysis of current and planned network designs and practices as well as consultation with legal counsel. For those that must become CALEA compliant, the FCC currently states that it will require “system security statements” to be filed at a date to be determined (no sooner than January 2007), and will require full CALEA compliance by May 14, 2007.

CALEA and Merit

Merit Network serves the high-performance networking needs of Michigan’s education and research communities. As an organization that provides Internet connectivity for other organizations, Merit will in all likelihood have to be CALEA compliant and create the requisite procedures and technical capabilities. Merit’s conclusions in this regard are independent from those of organizations that connect to Merit; each organization must reach its own conclusions regarding whether it must individually comply with CALEA. Merit Member and Affiliate organizations are neither specially bound to nor freed from CALEA compliance because of their relationship with Merit.

Merit will work with Members and Affiliates in the coming months to share information and to determine if, for example, Merit could serve as a “trusted third party” for organizations that must comply with CALEA. For more information, please contact your Merit support team.

A brief history of telecommunication surveillance

- At least since the Communications Act of 1934, courts have had the power to order various types of wiretaps at the request of law enforcement.
- Title III of the Omnibus Crime Control and Safe Streets Act of 1968 simultaneously outlawed the use of electronic surveillance by private parties and authorized its use —under court order—by law enforcement officials engaged in the investigation of specified types of major crimes.
- The Electronic Communications Privacy Act of 1986 (ECPA) extended the privacy protections and the wiretapping authority of Title III to a new set of technologies and services such as electronic mail, cellular telephones and paging devices.
- In 1994, the Communications Assistance to Law Enforcement Act (CALEA) was passed to specify the technical obligations communications carriers have in responding to wiretap orders.
- On March 10, 2004, the Department of Justice, FBI and Drug Enforcement Agency jointly petitioned the FCC regarding several aspects of CALEA, including a request that enforcement of the Act be expanded so as to ensure that communications carried over new media are equally subject to wiretap orders.
- On September 23, 2005 the FCC released its First Report and Order, concluding that CALEA “applies to facilities based broadband Internet access providers and providers of interconnected voice over Internet Protocol (VoIP) service.”
- In late 2005, various organizations (including ACE and EDUCAUSE) requested review of the FCC’s Report and Order from the U.S. Court of Appeals for the D.C. Circuit, arguing that the expansion of CALEA went beyond the FCC’s authority.
- On June 9, 2006, the U.S. Court of Appeals for the D.C. Circuit upheld the FCC’s new CALEA guidelines.

For more information

The FCC’s CALEA page:

www.fcc.gov/calea

The FBI’s “Ask CALEA” Web site:

www.askcalea.net

EDUCAUSE resource page on CALEA:

www.educause.edu/calea

Association of Research Libraries’ CALEA site:

<http://www.arl.org/info/frn/tr/calea>