



THE APPLICATION OF CALEA TO HIGHER EDUCATION NETWORKS*

In September 2005, the FCC issued an order extending the Communications Assistance for Law Enforcement Act (“CALEA”) to providers of broadband Internet access and interconnected voice-over-IP services. The U.S. Court of Appeals for the D.C. Circuit recently upheld that order on appeal. Unless and until a party obtains a reversal in a further appeal, the FCC order is the law of the land.

The FCC order briefly discussed the obligations of colleges and universities that operate broadband networks, and the Government’s court briefs and the court’s opinion provide further guidance. Generally speaking, a higher education or research institution should be fully *exempt* from CALEA if it satisfies two criteria: (1) its network qualifies as a “private network,” and (2) it does not “support” the connection of the private network to the Internet.

In practical terms, this means that an institution should be exempt where it restricts the use of its network to particular classes of users (e.g., students, faculty, and administrators), *and* where the institution relies on a third party (such as a commercial ISP or a regional network) to provide the transmission and switching facilities used to route traffic to the Internet, rather than self-supplying such facilities. Each criterion is discussed in more detail below.

1. What is a “Private Network”?

While CALEA exempts “private networks,” neither the statute nor the FCC’s rules define that key term. Without question, the term encompasses networks that are “closed” in the sense that they are self-contained and do not interconnect with a public network (either the Internet or the telephone network). The FCC’s order also strongly suggests that *interconnected* networks will be considered private when made available only to limited constituencies, rather than to the general public. Thus, campus networks that offer Internet connectivity but are made available only to students, faculty, and administrators—and that exclude the public at large, for example by requiring university ID cards to gain access to networked terminals and by requiring password authentication on wireless networks, among other measures—almost certainly would be considered private.

Many institutions provide some degree of network access—including access to the Internet—to members of the local community or the public at large (for example, at a computer terminal within a student center). While offering such access may serve other goals, it will significantly increase the risk that the campus network would be deemed “public” and thus

* The original version of this document, posted on July 13, has been modified slightly to avoid any suggestion that libraries are subject to CALEA.

subject to CALEA. It is possible that limited or incidental use by the public would not undermine the overall characterization of a network as private, particularly if the institution maintains a policy confining public access to a small number of network access points and allows it only during limited hours. Because the limits on qualifying as a private network operator have yet to be clarified or tested, however, institutions that seek to avoid any obligations under CALEA should adopt policies that prohibit public access to campus networks.

2. When Does a Private Network Operator “Support” the Connection to the Internet?

The FCC’s September 2005 order states that private network operators are exempt from CALEA unless they “*support* the connection of the private network to a public network,” such as the Internet. While the meaning of “support” is ambiguous, the Commission later clarified in the court proceeding that it “imposed CALEA obligations on private network operators that *provide their own connection* to the Internet but *not* on those that contract with an [Internet service provider] for that connection.”

This key distinction should mean that a college or university will be subject to CALEA only when it constructs, purchases, leases, or otherwise operates fiber optic or other transmission facilities and associated switching equipment that link the campus network to an ISP’s point of presence. Colleges and universities that rely on third parties to provide these connections should be exempt.

If a university connects its network to a regional research network, and that regional network also qualifies as “private,” that relationship should not affect the university’s exempt status. Moreover, the regional network itself should be exempt from CALEA if a commercial ISP provides the facilities that link the regional network to the Internet, whereas it would be subject to CALEA if it were to self-supply those facilities.

If a private network operator *does* provide its own connection to the Internet, CALEA will apply *only* to that connection point between the private and public networks. The D.C. Circuit Court of Appeals confirmed that CALEA cannot be applied to the internal portions of private networks, regardless of how they connect to the Internet. Entities that are subject to CALEA must ensure by May 14, 2007 that their “gateway” equipment provides the assistance capabilities set forth in the statute, including the ability to isolate a surveillance target’s electronic communications and call-identifying information. Providing such capabilities likely will require the replacement of existing gateway equipment or the retention of a “trusted third party” to provide CALEA solutions on an outsourced basis.