

New Responsibilities in the Post-September 11 World

In a speech dedicated to homeland security, President George W. Bush stated that the United States had entered a “new era” with “new responsibilities” for the government and the American people.¹ In helping the federal government fight this war against terrorism, higher education is being watched closely. Although college and universities have a tradition of cooperating with federal law-enforcement agencies, the reliability of academic computer network security has come under public scrutiny, especially since the high-profile hijacking of university computer networks for the launching of denial-of-service attacks two years ago. Many in the higher education community have voiced concern that colleges and universities will not be able to meet what they foresee as increased demands on IT staffs; others feel that by cooperating, institutions will be helping to attack the civil liberties that higher education nurtures.

Congressional Reaction: The USA PATRIOT Act

Under tremendous pressure from the White House and the U.S. public, Congress overwhelmingly passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (“USA PATRIOT”) Act of 2001,² which was immediately signed into law by President Bush on October 26. The USA PATRIOT Act contains several provisions of special interest to higher education, including sections on electronic surveillance and access to student records.³ Three areas are of particular interest to colleges and universities:

- The law modifies the Family Educational Rights and Privacy Act (FERPA) to expand the nonconsensual release of student records. Colleges and universities are not liable for cooperating in good faith with federal law enforcement, pursuant to a court order.
- The law expands the scope of technology-related information that law enforcement may obtain through a court order. It allows the use of “pen register”—or trap-and-trace—devices to obtain dialing, routing, addressing, or signaling information, if such information does not include communication content. As of this writing, it is unclear whether law enforcement will be allowed to monitor Web addresses visited by the computer user.
- The law authorizes communication providers to permit law enforcement to intercept communications of “computer trespassers” without a warrant. Users who have an existing contractual relationship with the owner or operator are not considered to be trespassers. Faculty, students, and campus employees most likely meet the contract criteria.

From a resource viewpoint, the USA PATRIOT Act imposes no new obligations on communication providers to provide facilities or technical assistance to law enforcement, and it authorizes financial



Illustration by Steve McCracken, © 2002

compensation for providing requested aid. However, some colleges and universities fear that if they do not conduct the requested monitoring, law enforcement will install its own monitoring devices (such as the FBI's surveillance software Carnivore), as allowed under the act. Not only are higher education network administrators loath to give up any control of their networks, but there is no guarantee that the information being collected is strictly that defined by a court order.

Privacy ramifications aside, how colleges and universities deal with the expansion of federal law-enforcement electronic surveillance powers may ultimately depend on the campus culture. For instance, not all higher education institutions require students to log on with IDs when using the campus computer system. Some defenders of this practice state that it protects the privacy of students who want to surf the Web in complete anonymity, allowing them to visit certain sites without fear that their Web habits will be made public. To ease compliance with law-enforcement requests, many IT administrators may be forced to rethink their computer user policies.

The electronic surveillance provisions of the new law will sunset in four years, by December 2005. This will allow the U.S. public the opportunity to convey any concerns to members of Congress as they consider whether to renew these provisions and, if so, whether to make any needed improvements. The higher education community must be vigilant during the next four years to record and report any perceived abuses by law enforcement when conducting electronic surveillance of campus communications networks.

Actions by Network Administrators

Given the stressful times, higher education institutions will face increased pressure to cooperate with law enforcement. Despite the wave of patriotism engulfing America, higher education IT network administrators must understand that they are under no heightened obligation to cooperate with federal law enforcement without a court order. Similar to previous communication-monitoring laws, the electronic provisions within the USA PATRIOT Act will most likely be

challenged in the courts if and when specific abuses are cited. In the meantime, network administrators are taking the following steps to ensure that they are complying with the new law and that they are securing their networks as best as they can:

- Conferring with the institution's legal counsel to make sure that everyone understands how the new antiterrorism law and any subsequent related laws affect the IT department
- Revisiting disaster-recovery plans—in particular, noting the lessons of colleagues directly affected by the September 11 tragedy at the World Trade Center⁴
- Redefining “IT security” to include not only the computer network but also how IT applies to the institution's physical security

As a complement to the resources within the higher education community, colleges and universities need to take advantage of the resources available within the federal government and local emergency agencies while working with them as equal partners.⁵ Federal agencies would appreciate the assistance of the higher education community in dealing with IT security issues. As the federal agencies scramble to shore up protection of communication networks, Congress is convening hearings on a wide range of security-related issues, including cybersecurity. Higher education must take an active role in these and other deliberations that will help to shape the future of cybersecurity on campus.

Notes

1. President George W. Bush, November 8, 2001.
2. Senator Russell Feingold (D-WI) cast the lone dissenting vote in the Senate after being denied the opportunity to amend the bill in order to address civil liberty concerns.
3. See the memorandum prepared by the American Council on Education's external counsel on the USA PATRIOT Act: <http://www.acenet.edu/washington/anti_terror/2001/2001_anti_terror.pdf> (accessed November 12, 2001).
4. See, for example, Frank J. Monaco, “IT Disaster Recovery near the World Trade Center,” *EDUCAUSE Quarterly* 24, no. 4 (2001): 4–7.
5. See the National Infrastructure Protection Center and other related federal agency Web sites: <<http://www.nipc.gov/sites.htm>>.

Garret Sern is a policy analyst for EDUCAUSE.

EDUCAUSE

Transforming Education Through Information Technologies

EDUCAUSE, a consolidation in 1998 of Educom and CAUSE, is a nonprofit consortium of colleges, universities, and other organizations, dedicated to the transformation of higher education through the application of information technologies. Through direct services and cooperative efforts, EDUCAUSE assists its members and provides leadership for addressing critical issues about the role of information technology in higher education.

EDUCAUSE Board of Directors

Ronald Bleed, Chair
Vice Chancellor, Information Technologies
Maricopa Community College District

Martin D. Ringle, Vice Chair
President, NorthWest Academic
Computing Consortium
Reed College

Amelia A. Tynan, Secretary
CIO and Vice Provost
University of Rochester

Joel L. Hartman, Treasurer
Vice Provost, Information Technologies
and Resources
University of Central Florida

Diane Balestri
Vice President, Computing and
Information Services
Vassar College

William H. Graves
Chairman and Founder
Eduprise

Joanne R. Hugi
Associate Vice President,
Information Services
University of Oregon

Gregory A. Jackson
Chief Information Officer
University of Chicago

Joel W. Meyerson
Director
Forum for the Future of Higher Education

Susan L. Perry
Director of Library, Information, and
Technology Services
Mount Holyoke College

Steven W. Relyea
Vice Chancellor, Business Affairs
University of California, San Diego

Donald R. Riley
Associate Vice President and CIO
University of Maryland

Ex Officio Member
Brian L. Hawkins
President
EDUCAUSE