

October 23, 2005

## Colleges Protest Call to Upgrade Online Systems

By [SAM DILLON](#) and [STEPHEN LABATON](#)

The federal government, vastly extending the reach of an 11-year-old law, is requiring hundreds of universities, online communications companies and cities to overhaul their Internet computer networks to make it easier for law enforcement authorities to monitor e-mail and other online communications.

The action, which the government says is intended to help catch terrorists and other criminals, has unleashed protests and the threat of lawsuits from universities, which argue that it will cost them at least \$7 billion while doing little to apprehend lawbreakers. Because the government would have to win court orders before undertaking surveillance, the universities are not raising civil liberties issues.

The order, issued by the Federal Communications Commission in August and first published in the Federal Register last week, extends the provisions of a 1994 wiretap law not only to universities, but also to libraries, airports providing wireless service and commercial Internet access providers.

It also applies to municipalities that provide Internet access to residents, be they rural towns or cities like Philadelphia and San Francisco, which have plans to build their own Net access networks.

So far, however, universities have been most vocal in their opposition.

The 1994 law, the Communications Assistance for Law Enforcement Act, requires telephone carriers to engineer their switching systems at their own cost so that federal agents can obtain easy surveillance access.

Recognizing the growth of Internet-based telephone and other communications, the order requires that organizations like universities providing Internet access also comply with the law by spring 2007.

The Justice Department requested the order last year, saying that new technologies like telephone service over the Internet were endangering law enforcement's ability to conduct wiretaps "in their fight against criminals, terrorists and spies."

Justice Department officials, who declined to comment for this article, said in their written comments filed with the Federal Communications Commission that the new requirements were necessary to keep the 1994 law "viable in the face of the monumental shift of the telecommunications industry" and to enable law enforcement to "accomplish its mission in the face of rapidly advancing technology."

The F.C.C. says it is considering whether to exempt educational institutions from some of the law's provisions, but it has not granted an extension for compliance.

Lawyers for the American Council on Education, the nation's largest association of universities and colleges, are preparing to appeal the order before the [United States](#) Court of Appeals for the District of Columbia Circuit, Terry W. Hartle, a senior vice president of the council, said Friday.

The Center for Democracy and Technology, a nonprofit civil liberties group, has enlisted plaintiffs for a separate legal challenge, focusing on objections to government control over how organizations, including hundreds of private technology companies, design Internet systems, James X. Dempsey, the center's executive director, said Friday.

The universities do not question the government's right to use wiretaps to monitor terrorism or criminal suspects on college campuses, Mr. Hartle said, only the order's rapid timetable for compliance and extraordinary cost.

Technology experts retained by the schools estimated that it could cost universities at least \$7 billion just to buy the Internet switches and routers necessary for compliance. That figure does not include installation or the costs of hiring and training staff to oversee the sophisticated circuitry around the clock, as the law requires, the experts said.

"This is the mother of all unfunded mandates," Mr. Hartle said.

Even the lowest estimates of compliance costs would, on average, increase annual tuition at most American universities by some \$450, at a time when rising education costs are already a sore point with parents and members of Congress, Mr. Hartle said.

At New York University, for instance, the order would require the installation of thousands of new devices in more than 100 buildings around Manhattan, be they small switches in a wiring closet or large aggregation routers that pull data together from many sites and send it over the Internet, said Doug Carlson, the university's executive director of communications and computing services.

"Back of the envelope, this would cost us many millions of dollars," Mr. Carlson said.

F.C.C. officials declined to comment publicly, citing their continuing review of possible exemptions to the order.

Some government officials said they did not view compliance as overly costly for colleges because the order did not require surveillance of networks that permit students and faculty to communicate only among themselves, like intranet services. They also said the schools would be required to make their networks accessible to law enforcement only at the point where those networks connect to the outside world.

Educause, a nonprofit association of universities and other groups that has hired lawyers to prepare its own legal challenge, informed its members of the order in a Sept. 29 letter signed by Mark A. Luker, an Educause vice president.

Mr. Luker advised universities to begin planning how to comply with the order, which university officials described as an extraordinary technological challenge.

Unlike telephone service, which sends a steady electronic voice stream over a wire, the transmission of e-mail and other information on the Internet sends out data packets that are disassembled on one end of a conversation and reassembled on the other.

Universities provide hundreds of potential Internet access sites, including lounges and other areas that offer wireless service and Internet jacks in libraries, dorms, classrooms and laboratories, often dispersed through scores of buildings.

If law enforcement officials obtain a court order to monitor the Internet communications of someone at a university, the current approach is to work quietly with campus officials to single out specific sites and install the equipment needed to carry out the surveillance. This low-tech approach has worked well in the past, officials at several campuses said.

But the federal law would apply a high-tech approach, enabling law enforcement to monitor communications at campuses from remote locations at the turn of a switch.

It would require universities to re-engineer their networks so that every Net access point would send all communications not directly onto the Internet, but first to a network operations center where the data packets could be stitched together into a single package for delivery to law enforcement, university officials said.

Albert Gidari Jr., a Seattle lawyer at the firm Perkins Coie who is representing Educause, said he and other representatives of universities had been negotiating with lawyers and technology officials from the Federal Bureau of Investigation, the Department of Homeland Security and other agencies since the spring about issues including what technical requirements universities would need to meet to comply with the law.

"This is a fight over whether a Buick is good enough, or do you need a Lexus?" Mr. Gidari said. "The F.B.I. is the lead agency, and they are insisting on the Lexus."

Law enforcement has only infrequently requested to monitor Internet communications anywhere, much less on university campuses or libraries, according to the Center for Democracy and Technology. In 2003, only 12 of the 1,442 state and federal wiretap orders were issued for computer communications, and the F.B.I. never argued that it had difficulty executing any of those 12 wiretaps, the center said.

"We keep asking the F.B.I., What is the problem you're trying to solve?" Mr. Dempsey said. "And they have never showed any problem with any university or any for-profit Internet access provider. The F.B.I. must demonstrate precisely why it wants to impose such an enormously disruptive and expensive burden."

Larry D. Conrad, the chief information officer at Florida State University, where more than 140 buildings are equipped for Internet access, said there were easy ways to set up Internet wiretaps.

"But the wild-eyed fear I have," Mr. Conrad said, "is that the government will rule that this all has to be automatic, anytime, which would mean I'd have to re-architect our entire campus network."

He continued, "It seems like overkill to make all these institutions spend this huge amount of money for a just-in-case kind of scenario."

The University of Illinois says it is worried about the order because it is in the second year of a \$20 million upgrade of its campus network. Peter Siegel, the university's chief information officer, estimated that the new rules would require the university to buy 2,100 new devices, at a cost of an additional \$13 million, to replace equipment that is brand new.

"It's like you buy a new car, and then the E.P.A. says you have to buy a new car again," Mr. Siegel said. "You'd say, 'Gee, could I just buy a new muffler?'"