A Walk Through the History of Southern Miss

Part 7

usmnews.net continues a new series revisiting nationally embarrassing events in the history of Southern Miss. As faculty, are your email communications private? At Southern Miss, the answer is no. What is the impact on academic freedom? While usmnews.net will not attempt to answer this question for everyone, many faculty tell our reporters and editors that they are "afraid" to use Southern Miss email accounts for any communications which administrators might find objectionable.

June 25, 2004

Who Owns Professors' E-Mail Messages?

By ROBERT M. O'NEIL

Resources: On electronic privacy

Related articles: View all of the advice and commentary from this special supplement on legal issues

By ROBERT M. O'NEIL

The recent settlement of a bitter controversy at the University of Southern Mississippi left one major issue unresolved. Two professors who had been openly critical of a high-level administrative appointee faced possible dismissal, and the president received a faculty vote of no confidence. The termination proceedings against the two faculty members were stopped after extensive negotiations, and the president remained in office. But the issue that won't go away, and that first surfaced at a mediation hearing between the professors and the university, concerns the privacy of a faculty member's e-mail messages. The incident raises, once again, questions about the legal status of electronic communications on campuses today.

During the hearing, which produced an otherwise satisfactory accord, the university's president stated that, after learning of the two professors' challenge to the credentials of the new vice president for research, he had directed a university lawyer to monitor the e-mail messages of certain faculty members. Such action, claimed the president, was appropriate because the faculty critics had "disparaged [the vice president] in an attempt to make her ineffective" and did so "with reckless disregard for the truth." His justification for examining faculty e-mail messages included allegations that the critics had misused state property and had undermined confidence in the university administration.

Faculty reaction to reports of that intervention was swift and predictably critical. Noel Polk, a professor of English who had followed the saga closely, expressed outrage at presidential surveillance of faculty communications, citing the action as a major reason for declining faculty confidence in the president. The central premise of Polk's position, and similar protests from other university professors, is one that deserves closer scrutiny: that faculty members' e-mail messages are private communications, to which the access of administrators without consent poses potentially grave threats to academic freedom.

Although the issue was hardly unknown to academic administrators when it arose at Southern Mississippi, it has received surprisingly little attention. The status of electronic privacy at colleges and universities first surfaced nearly a decade ago. Irene Wechselberg, a librarian at the University of California at Irvine, had taken medical leave. Knowing that Wechselberg might be out for some time, her supervisor asked for her e-mail password, which the librarian refused to disclose. The university administration, citing a pressing need to keep up with work-related communications, authorized the diversion of Wechselberg's e-mail messages to a colleague. Wechselberg exclaimed to a news reporter, upon learning of the diversion, "That's just an invasion of privacy." Eventually she sued the university in state court, asserting her privacy interests under the civil-rights clause of the state Constitution.

Other clashes were to follow. In the spring of 2002, Martha McCaughey, a professor at Virginia Tech, watched as campus police officers removed a university-issued computer from her office. The university justified that action by expressing its hope that her e-mail log might yield a source for a recent defacement of campus buildings. An administration spokesman explained that because the professor's computer was university property, Virginia Tech could search the hard drive without the faculty member's permission, adding that "the university reserves the right to copy or examine files on university systems." Similar statements or views could be found in the policies of most colleges and universities.

But are those policies appropriate and fair?

At first glance, it might seem that messages sent by electronic or digital means should be as private as those conveyed through more-traditional media. If a faculty member uses the university network to make a phone call, or sends a paper letter in a sealed envelope from the departmental mail room, the expectations of privacy are, properly, quite high. The phone call might be intercepted if, for example, an emergency demanded an interruption to reach either party. And the envelope might be opened if physical evidence -- the emission of a noxious chemical or an ominous ticking -- alerted the mailroom staff to a highly probable threat to person or property. But short of such exigent circumstances, privacy is the norm. We would not countenance an administrative

decree to tap phones or unseal and reseal paper envelopes because they might carry messages unsettling to the campus administration.

Yet e-mail communication is inescapably different -- and in obvious ways that would make a claim for perfectly parallel treatment seem naïve. For one, every user must enter a password to gain access to the system, thus allowing oversight by network officials in ways that a letter and phone call do not. Information-technology managers routinely back up some portion of every day's e-mail messages, thereby ensuring that not all such communications will remain completely confidential. Save for those few that are encrypted, most e-mail messages consist of plain text, and as University of Virginia policies wisely warn users, "they are like postcards in that others might view the messages in transit or those left in plain view." Such exceptions would not, however, forfeit the basic principles of privacy for most e-mail users. One could easily live with such variations if they represented the only recognized departures from confidentiality of personal communications.

The actual experience is, however, far different from such an expectation, and employees' claims for e-mail privacy have fared poorly in the courts. Two recent decisions illustrate just how far the current state of the law has taken electronic messages from their phone and paper antecedents.

Last year the U.S. Court of Appeals for the Third Circuit extinguished any lingering hope that the Electronic Communications Privacy Act forbade employers to divert and review their employee's e-mail messages. The appeals court rejected an employee's claim that his privacy was violated when his employer searched through e-mail messages that he had sent and that were stored on the company's computer system. Although the federal statute does forbid "interception," that ban applies only at the moment of transmission, and the law specifically exempts the "owner" of an e-mail system from any claim that employer access to employees' messages could constitute an unlawful "seizure" of stored messages.

The only source of hope seems to lie in state legislation. Connecticut law requires employers to at least notify their employees before gaining access to e-mail messages. In late May, the California State Senate adopted a bill that would require all employers to inform their employees of any monitoring of e-mail messages, and the measure awaits Assembly concurrence. (Earlier efforts to enact such a safeguard in California have failed on at least three occasions.)

Another recent and pertinent case specifically involves a university professor, but offers little hope that academic communications will be treated more favorably. Although the context was criminal prosecution for downloading child pornography -- hardly the most auspicious test case -- the court's disposition of the professor's privacy claim was nonetheless revealing. Noting with approval that campus policies "prevent its employees from reasonably expecting privacy in data

downloaded from the Internet onto university computers," the U.S. Court of Appeals for the 10th Circuit told the defendant professor that he "should have been aware network administrators and others were free to view data downloaded from the Internet."

Although the professor's e-mail messages were not an issue, and the material involved (child pornography) was uniquely unprotected, the court's disdain for such a professorial-privacy claim seems to transcend the facts of the case. The language, more than the outcome, cautions faculty members as "employees" to expect no special solicitude or protection from the courts.

As a result, institutional policies have become critical in defining the status of faculty members' e-mail messages, and there are compelling reasons for universities to provide greater protection for such sensitive communications than the law requires. Academic freedom should apply as fully to electronic or digital messages as to other media of professorial expression and interaction. Indeed, the rapidly increasing reliance on e-mail communication, not only for exchanges between faculty members but between professors and students as well, argues for special solicitude going well beyond the conditions of the factory or business office -- where the types of privacy concerns central to the academic environment, which warrant the special safeguards of academic freedom, are absent.

Ironically, even though the University of California system had not yet dealt with the diverting of messages during an employee's absence at the time of the Irene Wechselberg case, it was already far ahead of most other institutions in developing a computer-privacy policy. The current policy, which has been in place for several years and deals well and wisely with the Wechselberg issue, resolves e-mail-privacy concerns more fully than most others and offers a model as commendable as it is novel. It asserts that the university "respects the privacy of electronic communications in the same way that it respects the privacy of paper correspondence and telephone conversations." With certain narrow exceptions -- a Freedom of Information Act request or court subpoena, or carefully defined "critical operational circumstances" -- the policy requires that "an electronic communication holder's consent shall be obtained ... prior to any inspection, monitoring, or disclosure of the contents" of university-controlled electronic records. Where consent is not required, or time pressure prevents obtaining it, the university must at the "earliest possible opportunity ... notify the affected individual of the action(s) taken and the reasons for the action(s) taken." Finally, each campus must specify the process for "review and appeal" of any access or diversion that was allegedly authorized under any of the stated exceptions.

While the University of California policy may not be perfect, it is substantially more protective than those of most other institutions. Even so, an optimal e-mail-privacy policy might include a few additional elements. For example:

- The inevitable conditions under which privacy may be justifiably

breached should be fully detailed, as should the process by which "critical operational circumstances" are to be determined, and by whom.

- If time permits -- and it would be hard to imagine conditions so urgent as not to permit -- every effort should be made to alert the user so that he or she can seek legal counsel.

- The policy should make clear that where an intrusion or diversion does occur, the contents of any affected messages should not be used or disseminated any more broadly or retained for a longer time period than the basis for such action would warrant.

- A comprehensive computer-use and privacy policy should deal with myriad related questions -- like the terms and conditions of "acceptable use" materials that may validly be barred from being sent or received on university computers, the procedure for filing a complaint about an alleged misuse of the system, or the process for appealing any limitation imposed on access to the system -- and not simply those that have occasioned controversy or, in extreme cases, have landed the university in court.

A committee of the American Association of University Professors that released in 1997 a statement on Academic Freedom and Electronic Communications is revising that document and should issue a new statement in the fall that will also give some guidance on issues related to e-mail privacy. Given the certainty that such issues will arise ever more often, colleges should assess their own readiness to deal with electronic-privacy tests and frame or revise suitably sensitive policies. It is now clear that a University of California librarian on medical leave would have substantially greater e-mail-privacy protection than did Irene Wechselberg nearly a decade ago. What is far less clear is how well such an issue would be resolved at the great majority of other institutions, both public and private, at which privacy policies lag well behind those the California system was already developing at that time, and the completion of which was undoubtedly spurred by Wechselberg's lawsuit. It should not require similar litigation to get the attention of the rest of the academic world.

Robert M. O'Neil is founding director of the Thomas Jefferson Center for the Protection of Free Expression and a professor of law at the University of Virginia. He is the author of Free Speech in the College Community (Indiana University Press, 1997).