McCaughey, Martha. (2003) “Windows Without Curtains: Computer Privacy and Academic Freedom,” ***Academe*** 89:5: 39-42 (September/October). (ISSN: 0190-2946).

Windows Without Curtains:

Computer Privacy and Academic Freedom

Martha McCaughey

ABSTRACT: Focuses on the computer privacy of professors at public universities in the U.S. Details of a university police investigation using a professor's computer; Assessment of the moral limitation of computer searches on ownership grounds; Application of the Constitution's Fourth Amendment to the electronic environment**.**

A professor discovers the intricacies of electronic property rights when her computer becomes part of a police investigation. What rights do faculty have to work stored on a university's hard drive?

My friend caught her husband cheating. He used a car phone (it was the eighties). She had the car phone bill, which listed all the numbers he'd dialed, and one he'd dialed frequently enough to arouse her suspicion. So she called her local pizza shop, knowing they kept track of pizza deliveries by using the customer's phone number. She simply stated the suspicious phone number, in response to which the pizza guy confirmed the name and address--Hillary Homebreaker on 123 Deception Drive--where she then drove and made the bust. I celebrated the wife's ability to use computerized information systems to her advantage. Of course, the now ex-husband undoubtedly regrets the ease with which such information could be obtained. I have since learned a little more about life's technological regrets.

I'd always used information technology to my advantage. I've made a Freedom of Information Act request. I've created a Web page so that I could post a piece of criticism that my university's newspaper refused to print. I skated on the smooth side of the computer-age-old tension between the good and the bad uses of information technology. But when armed police officers confiscated and searched the computer from my state university office, without a warrant, I began to cross-examine my relationship to computers and investigate professors' computer privacy at public universities.

Space limitations prevent me from providing all the particulars of "Computergate," as the case came to be known locally, but here's the upshot: you could find yourself in the same position that I did. I had violated no university policy. I simply received an anonymous e-mail (an e-mail with a "from" line that read "Anonymous User" and an address of <anonymous@remailer.havenco.com>). The e-mail was the "manifesto" of a group claiming responsibility for having spray-painted antirape graffiti on the campus the day prior. The brief message defended the group's act of property defacement as politically necessary given the problem of rape. The manifesto indicated no future action or plans to deface more property or hurt people.

Because I directed the women's studies program, and such current events get discussed in our classes, I forwarded the message (with an explanatory preface) to my colleagues on our women's studies Listserv. I also forwarded to my colleagues a critique of graffiti as a form of activism, written by one of my students. The e-mail manifesto said that I was one of several people being sent the manifesto because I was perceived by the senders to be sympathetic to their cause. But I neither claimed nor denied any sympathy for their manifesto or form of protest. Nevertheless, I became virtual collateral damage.

In forwarding the e-mail to my colleagues, I attracted the attention of the campus police, who wanted the message to trace its origin and catch the senders/vandals. They called to ask me for it, and I offered to forward it to them. They explained that a forwarded copy would not be traceable to the original sender. I'd only kept a forwarded copy, however (the one I received from myself when I sent the message to the Listserv). I didn't know who else had received the e-mail (I have since learned that at least twenty people on campus received it), but I figured the police would check around and get a copy of it from a recipient who hadn't yet deleted it. But that isn't what happened.

Some days later, a campus detective called, asking for my entire computer to perform an e-mail recovery operation. I said he did not have my permission to take my entire computer and that I was about to leave town to see my father, who'd become critically ill. The day I returned, I found two police officers at my campus office to confiscate my computer. The request had become a demand. I asked them for a warrant. One officer said that they did not have or need a warrant, because the computer was university property. He said I must touch nothing, print out nothing (not even the paper I was writing under a publisher's deadline), and shut down the computer. My files for which I hold the copyright and in which I have intellectual property fights were not "university property," I protested. They conveniently ignored any distinction between the machine and the electronic files.

The university also later ignored that distinction when police and public relations officials told inquiring minds that the police had returned the computer a day later. They neglected to mention that the police officers had made a copy of the entire contents of the computer's hard drive. They copied thirty gigabytes of information for a four-kilobyte e-mail file--over 7.5 million times the information they needed. They also neglected to mention that the police made this copy after looking through some of my documents. For weeks, people would ask if I got my computer back. The answer was yes, but no.

When I got my copy of the hard drive back (police kept another), I used technology to do my own form of surveillance of my hard drive. I found that some of my files had been opened, including, for example, those saved as Pervert Evol Narr-Conf Version, WS Pictures, and Sex Toy Parties McCaughey. The documents were all part of bona fide research projects, most of them published already. The article on women's sex-toy parties was published in the academic journal Sexuality and Culture. WS Pictures was a backup file of online images of illustrious women--in their clothes. I couldn't help being shocked that my academically legitimate files looked like obscenity. After all, it's not as if my computer contained files with titles like WSNakedPictures or Pervert under 18.

Other documents on my computer--and on yours, too, I'm betting--might look suspicious to prying eyes. After all, most of us receive spam e-mails of all kinds. Whether it's the penis-enlargement spam, the Travelocity spam, or the Nigerian-money-scam spam, we are not in complete control of what ends up on our computers. I routinely receive sexually explicit jokes and political commentaries from friends, colleagues, and creepy fans of my scholarship. I don't particularly care for these messages, but unless I find a way to clean such files off my hard drive, they're on there. Usually, I'm too busy working as a professor to PC my PC. I don't even have time to wash out my coffee cup.

That the work I do--which I was appointed to do and which I do well and ethically--was suddenly the object of police scrutiny left me confused and anxious. For days, I worried about what would happen next in this Kafkaesque investigation: Am I going to be fired on specious obscenity charges? Was something wrong with having published an article on women's sex-toy parties? Am I under investigation for something? Am I being punished for something? What are my confiscated files doing out there without me? These questions gnawed at me for the entire thirteen months that my files remained with the police.

I'll leave aside whether or not any evidence gleaned from files obtained this way would have stood up in court--although this important question will surely emerge in future cases. As it happened, university specialists recovered that deleted e-mail but were unable to trace it to any sender's computer, since it was sent from an "anonymizing remailer," which is not traceable. So they never had occasion to use any e-mail or other file from the computer formerly known as my computer as evidence in any criminal trial. I was never arrested, fired, or reprimanded on obscenity or any other charges.

Yet the confiscation of my computer files not only caused anxieties about the Agents of Oceania convicting me of a thought crime. It also felt like a major intrusion, a violation. I'm a writer. I put my most cherished thoughts into that computer, articulate my toughest arguments, and

passionately invest my hopes and ideals. I communicate with and through it. To have it taken away from me was like being subjected to some form of sensory deprivation.

To have it searched left me with a real sense of worry not only about myself but about my current and former students. What sort of compromise in confidentiality does this pose to them? How are they feeling, and how might this change my relationships with them? Did they really believe that the papers they wrote, many of which they turned in by e-mail or through course Web sites, belonged to the state? How about the comments with which students entrusted me over e-mail--including personal information about being mentally ill, HIV positive, physically abused, or addicted to illegal drugs? I imagined my students having technological regrets upon hearing about the seizure of my computer and the university's position--stated to the press but not in any existing policy--that the university owns not just the computers but also everything on them.

Computergate opens a virtual Pandora's box of questions about our relation ships with, ownership of, and access to digital information in our increasingly electronic workplaces. We need to engage actively, perhaps even aggressively, the legal and bureaucratic architecture surrounding how we interact with computers. Public universities and other state agencies could attempt to redefine people's relationships with their computers, construing them as little more than surveillance tools or de facto bugs. Those of us who value academic freedom must push for open dialogue about what the computer means to us as university workers. We must also discuss matters of ownership and access.

Sometimes ownership matters, and sometimes it doesn't. The reliance on computers at work has changed the rules for employees and supervisors. Most faculty would assume that an employer or police officer cannot enter an office, confiscate, and then photocopy, the notes an employee wrote on her work-provided paper, but many defend the same action when the notes are intangible, electronic files. Most would regard the words on a page as different from the (employer-provided) ink used to write those words, but many still do not know whether having used a state-owned computer makes the words created one's own or someone else's. A pre-computer-age employer who suspected that her employee was slacking off would have had to confront the employee. Should such employers today be allowed to wait until the employee has gone to lunch and start nosing through his e-mails to see what he's been doing? Would we accept that the employer could also install a small camera and watch what the employee does? Should the university be a different kind of employer?

Although concerns about worker productivity are valid, it is plainly naïve to suggest that workers should not make any personal communications at work. We all inevitably play a social and a professional role at work: we celebrate employees' birthdays, we boost morale by throwing office parties, we announce the births of children and grandchildren, we collectively grieve the death of co-workers, and we even arrange lunch and social outings with people--precisely because establishing personal connections in addition to professional ties is good business for the university. In short, we treat people like human beings. At least I hope we do.

Beyond issues of snooping, we must consider whether the electronic files a person generates count as her property or as the property of the university administration. You may have written

something in your spare time and stored it, along with other work-related items, on the computer provided at work--as innocently as you'd stick a bottle of aspirin in one of your employer-provided desk drawers or display a family photo on an employer-provided bookshelf. What makes a family photo on your computer, as a screen saver for example, any different? Does putting that family photo on the computer suddenly make it state property if the photo on the bookshelf does not become state property?

More significant, some professors work as private consultants using their university-provided computing equipment. Some departments endorse such private consultancies precisely because doing so enables them to retain the most talented and well-funded faculty members. The employer provides the electronic equipment on which we work, but does that mean the employer owns the electronic files we created, including files associated with a private consultancy?

Intellectual property policies parcel out ownership in specific ways to specific university actors. But even if they did not, I suggest that computer searches must be limited as a matter of policy--regardless of which files the state thinks it owns. Justifying computer searches or seizures on ownership grounds has severe moral limitations. It diminishes worker trust in employers, productivity on the job, and the climate of academic freedom. Saying that the state has a right to seize and search an employee's computer files simply because it owns the computer is like saying a man gets to rape his wife simply because he's her husband.

Regardless of where you come down on the issue of who owns which electronic files, the issue of access to those files must therefore be settled. The human resources department of the state in which I worked created a policy saying that employees at state agencies cannot expect privacy in their electronic files. Although many of my colleagues reacted to this policy with a sense of chilled helplessness, the policy hardly gives law enforcement gratuitous access to employees' computer files. Indeed, individual state agencies can still decide the who, what, where, when, why, and how of computer privacy and access.

We can also apply the Fourth Amendment to the electronic environment, bearing in mind its intent to protect us from unreasonable search and seizure. In many cases, the courts have told us that in order to make a Fourth Amendment claim that one was subject to an unreasonable search and seizure, a person must have a reasonable expectation of privacy. How should the Fourth Amendment apply to professors? Should it apply to cases involving computer files in our locked offices or to documents transmitted electronically across university networks? Indeed, it is as yet unclear how such questions will be answered for the electronic files of professors (or other state employees). But let me use myself as an example. I'd say I had a reasonable expectation of privacy in my computer files, given that they were stored on a computer in my office, which was assigned only to me and to which I had a key. Sometimes I stayed at my office all night working and fell asleep, face huddled into a pillow I kept there for just such occasions. I had a reasonable expectation that, unless it was 5 A.M. when the building janitor made his rounds to empty the garbage from each office, nobody would wake me up. The solitude I enjoyed in my individually assigned, locked office was so great that even the police officers had

no way to enter it aside from urging the department secretary to use his master key to let them in.

In addition to the solitary physical space enjoyed by the machine and me, I used a personal identification and password to get into my e-mail. It's true that technology is such that the privacy of electronic communications cannot be guaranteed, but the personal access and password gave me a sense that the messages and files sent to me were intended to be receivable only by me. Further, when I logged onto my computer, created a new document, or sent an e-mail message, no banner appeared on my computer screen telling me that what I was about to create, send, or receive was state-owned or state-searchable information. Finally, my Word files are not up for public view in any shared folder or otherwise attached to a computer network, on campus or elsewhere. Hence I had no reason to assume that anyone else could or should view my files, particularly those that never traverse the Net.

What reasonable professor in this position would not have experienced the police confiscation and search of computer files as surprising and intrusive? It's not that professors expect to work in secret; indeed, we routinely publish our work and account for our activities. But while we do this work, increasingly on a computer, we do expect to be left alone. Consider the regulations and the freedoms in the predigital workplace. Why should we expect that our department chair will read a letter we send by e-mail if we don't expect her to read a letter we send out through the office mailroom? We must not let the PC kill our expectations of privacy.

In "Academic Freedom and Electronic Communications," a report published in the July--August 1997 issue of Academe, the AAUP suggests that e-mail messages to and from university professors be treated like regular mail, which is considered private even when we send it out through the campus mailroom. The report offers helpful guidelines for those creating computer privacy policies. The AAUP was, however, perhaps overly optimistic about academic environments in not foreseeing the possibility of law-enforcement agents doing computer seizures and searches without warrants. It is already difficult for a department head, dean, or provost to justify suddenly taking a professor's computer or files. Campus police officers' doing so poses particularly grave concerns.

Allowing the police unfettered access to files stored on university-provided computers at state schools compromises free speech and academic freedom more generally. It threatens our international colleagues, both professors and students, even more than it threatens me, a U.S. citizen of European descent. What if several professors of Iraqi descent received an anonymous e-mail message containing political arguments critical of U.S. foreign policy or claiming responsibility for anti-U.S, graffiti? If receiving a spam message about antirape graffiti generated the intrusion that it did, what level of intrusion will be considered justifiable in this arguably more extreme hypothetical circumstance?

Computergate was a chilling welcome to a new McCarthyism, a McCarthyism not run by a centralized political authority, but enabled by a specific way of understanding and treating computer technology. This "McCarthyism 2.0" serves as a wake-up call. I've spoken to many professors who mistakenly think that having an acceptable-use policy for comnmnications systems is the same as having a privacy or access policy. Some assume that capricious

computer searches, whether by police, a department head, or other employee, wouldn't happen on their campuses. I like to imagine that my now ex-university regards what happened to me as a technological regret. I do not regret working on a state-provided computer any more than I regret teaching in a state-provided classroom building.

The answer is not to advocate faculty members' bringing their own private computers into work, leaving their campus offices to work in their own homes, or using encryption software. Such strategies sidestep the real problem. An expectation of privacy does not require scholars to sit in offices with the curtains drawn across their windows; drawing curtains on their computer Windows should not be required either. Storing data on one's own privately purchased external hard drive could erode workplace privacy rights by indicating one does not have a subjective expectation of privacy unless one works on a privately purchased computer. Nor is the solution to keep your PC clean of any personal or non-work-related information (another strategy that concedes access to or ownership of electronic files to the state). Some of us simply cannot PC our PC because our work is that which might appear inappropriate (as in my case), or that which is personal (a professor writing an autobiographical poem, for example, or responding by e-mail to a student in crisis), or that which arouses political suspicion (a professor researching Islamic cultures, for example).

Do we really want to--and can we--write, teach, conduct research, and serve the public and our profession with a constant consciousness of an administrative or state presence? We must create or revise our universities' policies to ensure that the electronic environment enhances, rather than erodes, academic freedom and civil liberties, lest the P in PC change from Personal to Police.