This paper was presented at the 1995 CAUSE annual conference. It is part of the proceedings of that conference, "Realizing the Potential of Information Resources: Information, Technology, and Services--Proceedings of the 1995 CAUSE Annual Conference," pages 2-5-1 to 2-5-13. Permission to copy or disseminate all or part of this material is granted provided that the copies are not made or distributed for commercial advantage. To copy or disseminate otherwise, or to republish in any form, requires written permission from the author and CAUSE. For further information: CAUSE, 4840 Pearl East Circle, Suite 302E, Boulder, CO 80301; 303-449-4430; e-mail info@cause.colorado.edu.
The 1990s Challenge of Insulating the Institution with 1980s Information Technology Policies

Susan Stager, Ph.D., Indiana University
Virginia Rezmierski, Ph.D., University of Michigan
Tad Pinkerton, Ph.D., University of Wisconsin

The following document is a snapshot of the current policy environment at universities and colleges, the issues that are arising and are being debated. Many universities that have put policies in place to guide community functioning, are reviewing those policies to ensure that they are sufficiently robust to meet the challenges of the fast expanding and changing technology. While review of old policies is going on, new policy areas are also being identified and analyzed. New issues arise, partly analyzed issues continue to be discussed, partly approved policies wind their way through processes, and old policies continue to be in need of review. All exist within campus communities at the same time. Some policy issues even become obsolete before they go to press.
The 1990s Challenge of Insulating the Institution with 1980s Information Technology Policies

Susan Stager, Ph.D., Indiana University
Virginia Rezmierski, Ph.D., University of Michigan
Tad Pinkerton, Ph.D., University of Wisconsin

Introduction

Rushed to the implementation stage in the 1980s, IT computer use and security policies may appear flat, stilted, and superficial. The principles upon which these policies were built are still key ones, however, and the appropriate foundation for policies in the 1990s. What requires interpretation is such cosmetic phrases in these policies as "computing resources should be used in accordance with the high ethical standards of the university community." What does this and similar phrases mean in the 1990s?

As this paper is being written, we await the fate of the Cox-Wyden Amendment to the telecommunications deregulation bill. The amendment forbids the FCC from regulating Internet content. It also provides some liability protection for Internet service providers like colleges and universities if a good faith effort is made to prevent distribution of obscene material. This amendment symbolizes the moving target of legal and ethical solutions to problems encountered by colleges and universities as they provide Internet service to their campus community. One moment we think we have a clear reading on Congressional intent, the next moment a new amendment is introduced.

The following document is a snapshot of the current policy environment at universities and colleges, the issues that are arising and are being debated. Many universities that have put policies in place to guide community functioning, are reviewing those policies to ensure that they are sufficiently robust to meet the challenges of the fast expanding and changing technology. While review of old policies is going on, new policy areas are also being identified and analyzed. New issues arise, partly analyzed issues continue to be discussed, partly approved policies wind their way through processes, and old policies continue to be in need of
review. All exist within campus communities at the same time. Some policy issues even become obsolete before they go to press.

I. Historical--Yet Still Around--Policy Issues

There are policy issues that we have faced in the past which continue to need attention on university and college campuses. The following section identifies some of those issues.

A. Harassment
The populations of universities and colleges are made up of a high percentage of young adults. Many are experimenting with and/or refining new ways of communicating with their peers and with others. Technological changes cause all of us, regardless of age, to learn new ways of using the technology to get our messages across to others. In this fast changing arena we all respond at times without thinking carefully about the impact of our words. We all struggle with how to enhance our messages with the nonverbal cues that we use so readily in our face-to-face communications. We all need to be aware of, and responsive to, the personal boundaries of others and when and how we may violate those boundaries during communication.

Harassment, insults, hurtful, insensitive language, are all found in everyday communication. What is new, is the speed with which we can pass such forms of language to many individuals, and do so with anonymity in some cases. What are the new forms of problematic communication that we see on campuses as information technology is used? What constitutes civil communication? When and how are boundaries crossed in interpersonal communications? When is a message a harassment? All of these issues need to be examined and community values regarding interpersonal communication strengthened on a continual basis within university and college communities.

B. Pornography
IT policy makers still struggle with the question of what is pornographic. Community standards within the ivory tower differ from those without. IT policy makers should watch other media -- newspapers, film, video,
cable, TV -- for trends. For example, a recent issue of EDUCOM Review reports that Time Warner Cable wants to “scramble” sexually explicit programs on its New York community access channel, and make subscribers request programs in writing. The ACLU has charged “censorship.” Time Warner countered that it has the same right to control what it sends across the wires as the newspaper has to control what it prints. What control does IT have over its wires?

C. Copyright
Many students come from an environment in which copying music and videos is the norm. Many students believe that they are 'authorized' to copy any material that they require for their academic work. They equate student status with a special class of citizenry that can use information resources without cost.

The typical computer use policy contains a catch-all phrase with wording like the following: "Computing resources may not be used for illegal purposes. Examples of illegal purposes include: Unauthorized copying of copyrighted material." The student is no wiser after reading the statement than before.

The copyright issue is no less murky from within the walls of the computer center than outside. Copyright laws may protect program text, but it does not protect industrial design elements of the programs, such as command hierarchy in the Lotus v. Borland, case or the internal interfaces involved in the Altai v. Computer Associates case. (Communications of the ACM 1995) Copyright issues will continue to need attention and study.

D. E-Mail Privacy
Electronic communications are sweeping the campuses as the primary use of the technology. Electronic mail is used for interpersonal social communications, for the scheduling of meetings, for informal discussions of topics between staff, for discussion of highly sensitive and personal topics, for generally open and free discussions of public topics, and for decision-making at some levels. Most disturbing is the fact that like most forms of communication there is a mix of several of the above content
types within many messages. Individuals use the tool to accomplish a number of objectives at one time.

Some of the communications that travel across electronic mail are strictly business related; many are not. Some institutions have provided electronic communication tools explicitly for the purpose of increasing open communication and discussion, for increasing the exercise of Freedom of Speech, for creation and play with ideas, and for increasing the intimacy of groups. Some have provided electronic communication tools explicitly, and perhaps solely, for business functions.

The law is unclear as to the privacy of electronic communications. Should universities and colleges monitor the use employees make of electronic mail? If someone complains about a message received by an employee, does the employer have the obligation, the right, to intercept and read communications? As we keep records of the amount of use of systems like electronic mail, is there information in those logs that could be analyzed to identify the amount of time individuals spend in use of e-mail or even the specific individuals with whom they communicates?

II. Current Policy Issues Gaining More Attention

A. Social Security Numbers as Common Identifiers In this section we identify those issues which are currently being debated because they have taken new form through the use of technology.

Periodically, the issue of a single card/number which will identify individuals, a common identifier, arises. Over the years, often from the initiation of an effort such as in the case of social security numbers, leaders initiating the effort have insisted that the number will not be used for purposes other than that originally intended. However, in each case, once established, the number/device becomes embedded and found to be useful for many other purposes; it is readily adapted and reused.

Will universities and colleges face legal action from those who wish to protect their financial and other personal information, as uses of social security number continues to proliferate? Will a unique number be used on
college campuses, one that is not tied so directly to personal financial and credit information? Or will the increasing use of debit cards on the campuses cause the use of identification cards, cards tied to social security number and other personal information, to expand well beyond what is currently imagined? Will the momentum and ease of the technological applications using these common numbers, overshadow the privacy concerns in the use of common identifiers?

B. Liability for E-mail Campus Directories v. Paper Campus Directories
Suffice it to say that many universities now have a process in place whereby a student, faculty, or staff member may have an "unlisted" e-mail address, comparable to an unlisted telephone number. Are campuses giving individuals choices in this regard? Are they allowing privacy in large national and international arenas, but public information in local arenas if that is desired by the student, staff, or faculty member? Or are system applications designed in such a way as to be automated without user choice, or to be inflexible to different needs at different levels of information dissemination? What are the liabilities as we handle this type of personal information--directory information?

C. E-mail Stalking
The crime of stalking received national attention several years ago because of a few celebrated cases, especially that of David Letterman. The crime of stalking has found new expression on the campus network. One university has had a case in which the activity of a computing-intensive female student was monitored by a male via VMS software listing the terminal of logged-on users. No physical contact was made between the stalker and the female, a condition of most stalker statutes currently enforced. But the motivation of the individual was the same as that of the traditional stalker, and the police acted.

D. E-mail Bombs--Box Stuffing
Minimal programming skills are necessary to create a program that will generate enough junk mail to flood a mail box and shut it down. Is it a form of harassment, a harmless prank, an act of vandalism, a problem with impulse control, an educational problem, or a serious threat to system security that one user can close down access, for another, purposefully? What does the university or college say to users about
equity of access, about reliability of access? What is university responsibility in this regard?

E. E-mail As the Core of Lawsuits
Thanks to Newsweek, Time, and other popular media, the public now recognizes that a deleted mail message isn't necessarily an unrecoverable piece of evidence. The critical piece of evidence in a lawsuit may be an e-mail message retrieved by a university staff member from a server or back-up tape. The absence of a message on a back-up tape can be just as useful to a case.

In the commercial world, computer system detectives are hired to search for discarded files and messages, or even reformatted hard disks. To what lengths should computer center staff go to retrieve data to assist university legal counsel or local law enforcement officials? How much staff time should be devoted to the task? What should users be told about back-up files and other storage media? What is available under the Freedom of Information Act, even if it is not sought through court order? Can we maintain electronic mail privacy for users? How important is it?

F. Political Activism Using the Campus Computer Resources
At one university, the fine line between politics and Free Speech on the campus network first became apparent when the electoral board fined one of the student political parties for using e-mail communications during the student presidential race. The next volley was fired during the city/county elections when a faculty used a distribution list to send an endorsement of candidates to his friends on campus. The next step was a request from a state representative to have a home page on the University system. Each step of the way there was debate about the proper role of the University.

Another form of political activism that may affect universities is of the "Tiananmen Square" variety. Students may involve the computer network in their struggles with administrators. While in the 1970s students brought universities to their knees by flushing all of the dorm toilets simultaneously, students could easily bring the campus computer system to its knees as well. When 4,000 people attempted to log into Goodard Space Flight Center to see comet Shoemaker-Levy hit Jupiter in 1994, the
system, designed for 30 simultaneous users, crashed. Campuses are already feeling the strain of scaling up to the number of simultaneous users that want to use the increasingly popular tools. Campus networks can crash with, or without, a political motivation.

III. Emerging Policy and Debate Issues

New issues arise almost daily as technology is being applied in new and modified ways. The issues identified in this section are just beginning to be debated on university and college campuses. Few policies are in place to guide communities in these areas as yet.

A. Digital Signatures
In the not-too-distant future, we will be amazed that we ever debated the validity of on-line signatures. In the Middle Ages it was necessary that heated wax, in the form of a symbol, be affixed to a document. The symbol might be the family seal embellished with mottoes. Today, our legal system finds that a promise can be binding without a written signature. Those of us who have performed the bulk of our work electronically for some years now, daily use our plain-text ASCII name in the e-mail "from" line as a symbol of our promise. And as time passes, we are more and more comfortable handling major business transactions with digital signatures. This society long ago dispensed with the seal as a sign that a promise would be enforced. Are we building adequate devices to ensure that a signature is what we believe it to be, and made by whom we expect?

B. Racial Electronic Terrorism
In October of 1994 someone broke into the computer account of a Texas professor and sent racist messages to about 20,000 computer users in four states. In response, about 500 users sent the professor death threats and other harsh responses.

Messages, felt to be racist or otherwise threatening and obnoxious, can be sent, responded to, forwarded, and many times duplicated without ever confirming the source of the original message, without identifying the actual sender. What is the role of education on campuses in these matters? What do we need to do to develop systems that help individuals confirm identities of senders of messages, or at least understand when
forged mail is received? What role, if any, do universities and colleges have in protecting their users from such acts of indirect terrorism?

C. Commercial Ventures on the Internet
With over 700 electronic malls and specialty stores on the Internet, all accessible from your campus computing network, it is difficult to enforce a campus policy of "no commercial use of the campus network." What is the purpose for which the campus network was created? Is it important to justify the use of the funds and try to restrict the commercial use of the network? Is expansion of the use of the campus network to non-affiliated users a natural, extension of service, solely driven by the potential of a new source of funds, or a needed extension of service to wider communities? Or is it a misuse of funds and an inappropriate intrusion into the life of the campus?

D. Authoritative Source for On-line Documents
With the immense popularity of the World Wide Web, and the desire of so many users to display documents in that environment, a significant question regarding representation comes into focus. What documents on the WWW represent the University? How does an institution confirm the validity and integrity of documents that purport to represent the University? What is the authoritative source for information? How does the institution organize and manage the input and updating of significant documents that represent their campus?

E. Institutional Records in the Electronic Environment
As administrators, faculty, and staff of universities and colleges create more and more documents within the electronic environment, and store them in different forms, identifying and preserving records becomes an important policy consideration. Who creates records? In what format or medium should records be created? If they are contained within electronic communications, how can record and non-record content be separated? How can the institution guarantee that documents that are created electronically, and perhaps stored electronically, will be available one year from now when, perhaps, systems are changed and information is transferred from place to place? How will the institution guarantee that the documents will be readable one year from now when, perhaps, the tools have been upgraded or discontinued? What should the operational
policy be within universities and colleges to ensure the creation, maintenance, and preservation of university records?

F. Handling of Personal Information
We are now able to pass information around the electronic environment of our institutions with increasing ease. Everyday it becomes easier to cross over the barriers caused by different technological platforms, and pass documents from one user to another. Administrators at many universities and colleges are talking about sending data between institutions over the networks. As each college and university faces these new potentials, they will need to examine the current and future practices when it comes to the handling of the personal information of members of their communities.

What is personal information? Is the newly digitized signature of an individual user the property of the University or of the individual? Can it be used in one or more ways? Did the individual understand the ramifications of giving that signature to be digitized? What about photographs? How can they be used by institutions? Do individuals understand the ways in which the University intends to use the photograph at the time that it is taken? Does the University even understand its own intent as it asks for this personal information? What will the universities and colleges do as they consider the possibility of transporting student grades, transcripts and other information between institutions? What policies will guide these decisions?

G. Image Alteration
Images are now possible to alter digitally without a trace. Photographs can so easily be changed that their use in court is being diminished. Soon we will be able to alter active video as well. What ramifications will this ability to alter images have on the campuses? Will altered images of a President of a University, for instance, be seen as Freedom of Expression or as character assassination? Will placing an individual in a scene falsely and publishing that picture be understood as misrepresentation, or artistic creativity? What are the policies and guidelines that will be needed to protect against impulsive administrative actions, and what will be needed to protect essential Liberties?

H. Libel Revisited
Colleges and universities remain uncertain as to their vulnerability for postings by students. An agreement was reached this month between the law firms representing Prodigy on-line services and Stratton Oakmont. Stratton Oakmont, an investment firm, felt it had been libeled on Prodigy when a user posted a message accusing the firm of “criminal fraud.” In the agreement, Prodigy would not be held libel.

Hopefully this court decision will be generalized and put an end to concern that the university will be held responsible for postings on its computer network. In a sense, this court decision grants the computing network the same status as the telephone network in that telephone companies cannot be sued for libelous calls made on its lines.

IV. Enduring Principles in Current Policies

While the issues are complex and ever-arising, there are some enduring principles which seem to be repeated as we continue to debate old issues, participate in the current discussions, and examine the new emerging issues. These principles help to clarify issues as belonging to various continuation of values on campuses. Once we are able to identify what the issues are really about, it becomes easier to accomplish the values clarification work that must be part of any policy development process. Below are some of the enduring principles.

A. Distinguishing Between Private v. Public Information
The debate between public vs private information is being played out at all levels. Historically, many documents have been made available to the public at selected sites, such as libraries, requiring the public to come to that site in order to access the documents. With the growth of the superhighway, at the state and federal government levels, statutes, administrative codes, and the text of bills being considered by the legislature (including the bill's status and what its fiscal impact would be) are being made available over the Internet. Some states, such as New York, sell the information to provide another revenue source for government. California is on the other end of the spectrum, making the information available at no charge to anyone who wants it.
At the University level, debate reigns about what is public and what is private information. State and federal statutes take some of the guesswork away. However, there is still a gray area. To further complicate the matter, statutes often use the terminology that public documents must be made 'accessible' to citizens. What does 'accessible' mean in the age of the Internet? Distinguishing between public and private information is a principle that will assist policy development.

B. Distinguishing Between Security and Ease of Use
The gap is widening between security on administrative computing systems and academic computing systems. At the same university, administrators may be required to transgress through three levels of passwords to acquire a database that is ultimately part of the same campus network used by students who routinely share their password with friends. Distinguishing between areas requiring security and those requiring ease of use is a principle that will benefit policy makers.

C. Distinguishing Between Institutional and Individual Ownership
The copyright laws are currently under revision, leaving the University in limbo on these critical issues. The complexity of copyright increases in the multimedia environment. The person who created the original work owns the copyright. Accordingly, the text might belong to the professor and the image might belong to the graphic artist. Yet in many institutions, the University owns the copyright for both because it employs both the professor and the graphic artist. Distinguishing between institutional and individual ownership in policy will provide guidance for communities.

D. Distinguishing Between Social Responsibility and Experimentation
Universities and colleges have a large investment in allowing free experimentation and creative expression on their campuses. Freedom of Speech is an imperative if we are to meet our missions of teaching, learning, and the creation of knowledge. But where does experimentation end and social harm begin? In this new electronic environment, how do we clarify the limits and boundaries of these concepts? Distinguishing between responsibility and experimentation and the limits of each, is an important principle for both policy making and for education.

Conclusion
The members of this panel have years of experience at their respective universities in contemplating the issues surrounding the use of information technology. They do not claim to have the answers to all of the questions raised in this paper or to those that will be raised during the panel presentation. However, they will share their thinking and the guiding principles that have helped them to cope with new issues. They will share advice as to how to deal with this exciting time for policy makers. They will look at 1990s challenges and the robustness of the 1980s policies that they have helped to create.