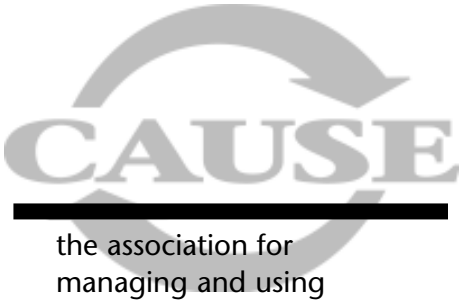


the association for
managing and using
information resources
in higher education

Privacy and the Handling of Student Information in the Electronic Networked Environments of Colleges and Universities

A white paper developed by a CAUSE task force in cooperation with the American Association of Collegiate Registrars and Admissions Officers

the association for managing and using information resources in higher education

4840 Pearl East Circle, Suite 302E
Boulder, Colorado 80301

phone: 303-449-4430
fax: 303-440-0461
info@cause.org
http://www.cause.org/

Foreword

Virtually all colleges and universities are learning to deal with the explosive growth of electronic networks, connecting every part of the campus community and linking to colleagues and information resources across the country and around the world.

As an association made up predominantly of information technology professionals, CAUSE has been especially concerned with the impact of such technology on the campus community. We're well aware that many of the issues higher education institutions are facing today stem from the proliferation of campuswide networks and Internet connectivity — issues related to free speech, censorship, student records privacy, ethical standards, managing "institutional information" on the World Wide Web, intellectual property, and copyright. And as campus technology administrators and chief information officers, our members are frequently expected to participate in — sometimes even to drive — campus initiatives to establish policy that addresses networked electronic information resources.

A key set of related issues revolves around the handling of student information, which under the Family Educational Rights and Privacy Act (FERPA) of 1974 enjoys special protection. In recognition that many of our members must deal with these issues, the CAUSE Board of Directors assembled a task force of individuals with diverse perspectives and responsibilities to identify and articulate, through a white paper, the privacy and confidentiality issues that arise regarding access to and transmission of personally identifiable student information in an electronic, networked environment.

Responding to this charge has not been easy. The members of the CAUSE task force found much to debate as they met for discussions that led to the development of this paper, clear evidence that the issues are complex and there are no universally agreed upon solutions. As the work of the task force progressed, new developments and perspectives fostered the realization that this is a moving target. Like the task force, so too will members of campus communities find diverse perspectives with respect to the values of privacy and information access at their institutions. What is important is the discussion and debate.

It is for this reason that this paper does not prescribe what policy should be for every campus with respect to privacy. Instead, it identifies the primary privacy principles involved, recommends a process whereby a full spectrum of campus constituencies can be involved in discussions that will lead to a better understanding of campus culture and values with regard to these principles, and suggests what might represent the lesser or greater application of each principle. In my view, this represents a significant contribution from which all CAUSE members can benefit — thanks to each member of the task force for a job well done!

To support a continuing dialog, CAUSE plans to create an electronic discussion forum for those who read this paper and wish to respond to the issues raised by the task force and their recommendations. For more information about this forum, check the "Hot Links" at the CAUSE World Wide Web site or inquire to info@cause.org.

Jane Norman Ryland
CAUSE President
April 1997

CAUSE Task Force Members

Task Force Co-Chairs:

Virginia E. Rezmierski (ver@umich.edu) is Director of Policy Development and Education in the Information Technology Division at the University of Michigan. An educational psychologist by training, she holds adjunct associate professorships in Michigan's School of Education and School of Public Policy. Dr. Rezmierski chairs the IT security committee as well as many committees that analyze ethical and legal issues. She has written policy for the University related to information technology since 1985.

Susan K. Ferencz (ferencz@indiana.edu) is Director of Policy and Planning for Information Technology at Indiana University, and has had major responsibilities in developing the student computing environment at Indiana for nearly ten years. She received her Ph.D. in educational psychology from Indiana University and currently attends IU's School of Law. She is a member of the graduate school faculty, usually teaching statistics. Ferencz is a member of the 1997 CAUSE Board of Directors.

Task Force Members:

Laurence R. Alvarez (laurence.r.alvarez@sewanee. edu) is the Associate Provost at the University of the South where he is responsible for all computing and telecommunications. He has been involved with computing and concerned about privacy issues since the early '70s. Sewanee's campus network reaching every office and student room was created in 1990 under his planning and direction. Alvarez is a member of the Board of Trustees and Treasurer of Educom.

Clair W. Goldsmith (c.goldsmith@cc.utexas.edu) is Deputy Director of Academic Computing and Instructional Technology Services at the University of Texas at Austin. He received his Ph.D. in Electrical Engineering from Southern Methodist University. Dr. Goldsmith also chairs the University of Texas System Information Technology Management Council. He participates in both technical and policy committees for UT Austin, the UT System, and the higher education industry.

Kathleen R. Kimball (krk5@psu.edu) is the Computer Network and Information Security Officer at Penn State University. She has over 20 years experience in researching, developing, testing, and evaluating intelligence systems, and in the security aspects of networked information systems. Prior to joining Penn State, she was instrumental in the development, implementation, and integration of security policy, procedures, and technology in support of NORAD and the U. S. Space Command.

Robert Morley (morley@mizar.usc.edu) is Associate Registrar at the University of Southern California where he has led a number of technology initiatives over the past 15 years. He also serves as a University advisor on matters related to FERPA, privacy, and confidentiality in the student records area. He is former chair of the American Association of Collegiate Registrars and Admissions Officers (AACRAO) committee on electronic data interchange (SPEEDE), and current chair of AACRAO's Task Force on Technology.

Trang Phuong Pham (trangp@umich.edu) will be receiving her master's degree in Public Policy this spring from the University of Michigan. She received her bachelors of arts degree from the University of Texas in Austin, and next plans to study law. She will be pursuing a career in intellectual property law, specifically copyright and trademark issues concerning the field of information technology.

Robert Ellis Smith (0005101719@mcimail.com) is publisher of *Privacy Journal*, a monthly newsletter based in Providence, RI, and the author of *Our Vanishing Privacy* (1993) and *Privacy: How to Protect What's Left of It* (1979). A lawyer and journalist, he was associate director of the Office for Civil Rights in the U.S. Department of Health, Education and Welfare with responsibility for higher education compliance in the 1970s.

Steven L. Worona (slw1@cornell.edu) is Assistant to the Vice President for Information Technologies at Cornell University. He has worked in the field of computer-mediated information storage and delivery for over 25 years, including development of CUinfo, the first campuswide information system. His technical responsibilities involve the award-winning CUPID network-printing system and the Cornell Digital Library. He is a director of Cornell's Computer Policy and Law Program, and serves on a wide variety of on- and off-campus technical committees.

NOTE: The task force asked a number of individuals with special perspectives and expertise to review this paper in its draft stage. *See page 49 for a list of those who provided valuable input in this process.*

Privacy and the Handling of Student Information in the Electronic Networked Environments of Colleges and Universities

I. Executive Summary

There is no turning back from the explosion of innovation and creativity the information revolution represents. Information is a powerful commodity which, used properly, can expedite, enfranchise, and enrich. However, misuse of the power of information can cause harm, especially with respect to individual privacy.

The recent shift to a networked information environment is challenging the protection of privacy in a number of ways. In colleges and universities, the focus on privacy issues has traditionally been on student records and the officials charged with responsibility for them — registrars, bursars, financial aid officers, admissions personnel, judicial administrators. But with the adoption of distributed technology architectures and widespread use of the network as a platform for instruction and student services, others in the campus community have also become stakeholders — faculty, deans, information systems developers, network administrators. And while these individuals may gather and store information generated by and about students or develop student-related technology applications, they may be unfamiliar with the unique legal, ethical, and policy issues related to privacy and the handling of student information.

Other key factors raising student privacy issues are:

✓ the increasing creation of information by and about students that does not reside in structured databases but results from systems or technology transactions or electronic communications;

✓ the ease with which information in electronic form can be accessed, manipulated, and transported; and

✓ the security of student information accessed or transmitted in a networked environment.

As institutions embrace information technology to enhance teaching and learning, streamline business processes, and improve student services, they are finding information technology to be both a bane and a blessing with regard to privacy. There is a delicate balance between the responsibility for maintaining student privacy rights and the responsibility for providing effective and efficient service to students. To preserve that balance, colleges and universities will need to engage in a process that examines basic principles underlying institutional values and policies related to privacy and information access. Enough technological change has occurred in the last several years to prompt a reevaluation of privacy policies created prior to the emergence of ubiquitous network technologies — policies that may have been overtaken by events — for possible adjustments. Or new policies may be needed where none currently exist. While this process should start with the legal implications of the Family Educational Rights and Privacy Act (FERPA) — the very foundation of student information practices — it is also important to consider ethical and policy issues, as well as institutional needs.

This paper recommends using a set of principles of fair information practice as a framework to guide such campus discussions, including:

- Notification
- Minimization
- Secondary Use
- Nondisclosure and Consent
- Need to Know
- Data Accuracy, Inspection, and Review
- Information Security, Integrity, and Accountability
- Education

These discussions should be open and institution-wide, bringing together many different stakeholders to determine campus values with respect to privacy and information access; to balance privacy rights with institutional needs and state and federal requirements; and to weigh the potential benefits of technology applications against the potential risk of privacy abuse.

Higher education as an industry has the unique challenge not only to respond to the cultural change occurring as a result of technological advances, but also to lead that change. Colleges and universities must prepare the next generation to fully understand both the tremendous potential embodied in new technologies and the responsibilities that accompany their use. Understanding the legal, ethical, and policy implications for privacy in a networked environment is an important part of that education — not only for students, but also for faculty, staff, and administrators.

II. Introduction

Seeking new and more effective ways to fulfill their missions, colleges and universities are rapidly increasing their use of computing and communications technologies. Technological advances have opened exciting opportunities to change teaching and learning paradigms — to reach nontraditional students and improve learning in traditional student populations; to create new and more dynamic business systems to increase institutional efficiency; and to deliver student services faster and more effectively.

The ability to deliver education "virtually" through the use of sophisticated communications technologies is breaking down traditional geographic barriers to competition, and many institutions are losing the geographic monopoly they previously enjoyed. In response to these competitive pressures, many colleges and universities are looking to technology to enhance marketability and allow them to reach distant learners.

In response to demands to streamline operations, many campuses are adopting new business models that promise to provide efficiencies and economies — models that cannot be implemented without investing in a campuswide technology infrastructure. For example, one reason many institutions have created distributed, networked environments is to support their strategy of decentralizing administrative functions — such as budgeting and purchasing — to enable more efficient conduct of business.

Most institutions are also exploring methods for giving their students electronic network access to their own grades, transcripts, course schedules, and other information. With students being able to register online, institutions expect to see a reduction in the time it takes students to enroll in classes and to drop or add classes, and a general reduction in paperwork. The goal is to streamline the delivery of student services, making student interactions with the institution more convenient.

The mission of higher education — the pursuit of excellence in learning, teaching, scholarship, and service — requires knowing a considerable amount about students: how well they are performing, where they live, what courses they are taking, and so on. Much of this information is a product of the educational process, some of it is a product of assisting the student with meeting educational requirements, and some of it is a result of simple transactions such as eating in a college or university dining room or checking a book out of the library. This set of information contains elements that an individual student may consider private. Further, associating some items with other items may create new information that may be considered private.

Beyond FERPA

Colleges and universities have an obligation to protect the confidentiality of student information. For more than twenty years, the Family Educational Rights and Privacy Act (FERPA) of 1974 has provided the foundation for handling student information within educational institutions (see Appendix A for a brief overview of this law). At the time of its passage FERPA was, and continues to be, far-reaching legal protection for the privacy rights of students.

That new technologies are being employed or that FERPA provides the legal basis for handling student records is not new. Nor is the fact that privacy violations occur — with or without technology. What is new, however, is the increasing complexity of the issues to be addressed when student information is handled within electronic networked environments.

Issues about handling student information are no longer limited to student records in structured databases such as grades, transcripts, and class selections. Many other pieces of information generated by and about students are becoming increasingly available because of network technology. For example, technology makes it possible to capture, store, and access medical information, digitized and stored photo images, and information about individual students such as their entrance to buildings, use of the library, the times and places they dine, when and where they sign on to computing resources, what they do once signed on, what they buy, and where they use their money cards. Though much of this information was available before the use of computers, what is new is the ease with which such data can be accessed and manipulated electronically by members of

the community, and perhaps by others, with both positive and negative ramifications. It is easier to combine databases, to perform automated search and sorting processes, to use data for secondary purposes with no human authorization, and to instantly transport data over electronic networks from one location to another — perhaps without a moment's reflection on the privacy implications of such actions.

Adding to the complexity are two other factors:

- the increasing distribution of student data and decentralization of authority for its protection. In today's networked environment, control of this information is no longer solely in the hands of the registrar and other academic officers, but is shared by others who may be unaware of privacy considerations in handling student information.
- the fact that process decisions (how systems work and how access controls are managed) and tool decisions (how information is formatted, displayed, and presented) are often based on purely technical criteria, sometimes without input from the "stewards" of the data that are to be managed within those systems. Privacy and security issues are often addressed as an afterthought. In the words of one registrar who provided input to our task force, " ... the responsibility for technology applications rests with people who have not had to be concerned with privacy and compliance issues."

An understanding of privacy is no longer limited to the legal implications of FERPA. Many colleges and universities recognize the need to also address the ethical and policy concerns that arise in a networked environment. New technologies are exposing campus administrators to a barrage of inquiries, demands, and complaints: "What is your policy in the area of X?" "I object to the use of personal information Y." "Please provide extract Z from your online database." Without comprehensive, carefully considered policy, the need for case-by-case decision-making will turn into an impossible burden.

The implications of networked technologies on the privacy of students, on the handling of personal information, on tradeoffs between privacy and service, and on the management of relationships between institutions and individuals are of such critical importance that they must be systematically examined by people with a diverse range of responsibilities institution-wide.

Notes another registrar, "A primary issue on our campus is the conflict between the values of privacy protection, convenience, control, and flow." Policy regarding privacy and networked information resources should be determined at an institutional level, and can no longer be determined by any single campus department. In their 1995 book, Alderman and Kennedy wrote:

> Whenever an invasion of privacy is claimed, there are usually competing values at stake. Privacy may seem paramount to a person who has lost it, but that right often clashes with other rights and responsibilities that we as a society deem important.[1]

This is at the heart of the dilemma facing colleges and universities. There are significant compelling, yet often competing, forces as they try to make decisions about how to move forward in implementing information technology. Tradeoffs and compromises must be considered. However, rights and responsibilities do not need to be at odds. Protection of privacy, enabling autonomy and intellectual freedom, and promoting civilized behaviors are important to communities of higher education and to learning communities in general, and new technology advances can provide assistance in such efforts. How can colleges and universities meet those objectives and take advantage of technological advances to meet institutional needs at the same time?

This paper was developed by a task force commissioned by CAUSE, the association for managing and using information resources in higher education, in cooperation with the American Association of Collegiate Registrars and Admissions Officers (AACRAO). The purpose of the paper is to:

- provide the reader with a framework for identifying and understanding the issues surrounding privacy and the handling of student information in an electronic networked environment,
- stimulate the clarification of values within institutions by encouraging discussion of privacy and technological issues, and
- provide guidance, resources, and a process for examining and creating policy to guide practice.

In developing this paper, our task force chose to look beyond the letter of the law to examine ethical is-

[1] E. Alderman and C. Kennedy, *The Right to Privacy* (New York: Alfred A. Knopf, 1995).

sues and information policies and practices not explicitly covered by existing laws.

The paper first examines new technological advances and ways they present both opportunities and pitfalls for privacy in the academic environment; then identifies eight principles our task force believes are important to policy development and fair information practice; and finally suggests a process that campuses can use for values clarification and policy development. Several appendices provide supplemental information including an overview of FERPA, definitions, recommendations and a checklist for policy and practices, additional information principles, information about sources of input to the task force, references, and resources.

III. Privacy Issues in an Electronic Networked Environment

Twenty years ago, except perhaps for a few scientists, people did not have computers in their homes. Similarly, only a few short years ago if someone had used the term "World Wide Web" one might have thought of spiders, or a creation by E. B. White. Yet today these are integral and irreplaceable elements of everyday life. There is no turning back from the explosion of innovation and creativity the information revolution represents.

While networked environments challenge the protection of privacy, they also afford opportunities to enhance privacy. Before examining in greater detail such challenges and opportunities, a brief discussion of the concept and importance of privacy is in order.

Throughout this paper, we refer to privacy as a right of individuals to control personal information about themselves (a right that in many instances is limited by other considerations). That right includes an opportunity to inspect information about themselves held by organizations and an expectation that the information will be accurate. We refer to confidentiality as the property, or characteristic, of information that is kept secret and secure. Organizations obviously have an interest in keeping information about themselves confidential, but, strictly speaking, that is not based on a right to privacy, which is an individual right.

The Importance of Privacy

Why is this individual right to privacy important, in particular to students on college and university campuses? Privacy is the foundation of the intellectual freedom that is critical in higher education. Especially critical for the growth of students is the ability to freely explore and communicate ideas and to be totally honest in forms of expression. Conditions must exist in which these activities may take place without stigmatization and without later consequences for participating in this world of ideas. Colleges and universities have a responsibility to create and to protect these conditions to facilitate and encourage the intellectual growth of students.

College is also a time of transition, pressure, and dramatic intellectual and emotional growth for most students. It is the time of breaking away from known protected environments, when students find themselves in unfamiliar territory. It is a time of exploring new social and intellectual environments in which they begin to define for themselves their more independent identities and routines. During this often unstable and vulnerable time, students may be unduly sensitive about their heritage, their strengths and weaknesses, their families, the look of their bodies, their disabilities or illnesses. Providing an environment where privacy is possible and information about themselves can be controlled eases one of the many pressures of campus life.

In a learning environment, students need to be independent — to have a sense of autonomy in asserting their beliefs, ideas, and values. Privacy is the foundation for such self-governance and autonomy. Without the ability to control and release information about themselves at will, students can become more vulnerable to the desires, assumptions, and power of others. They may also be hurt economically, educationally, socially, or psychologically by information theft or misrepresentation. The incident below illustrates how information can be used to draw assumptions and perhaps to disadvan-

tage an individual, reducing his or her autonomy.

> One of the largest distributors of credit cards in the country at one time had the practice of routinely denying credit cards to students majoring in history, English, and art. They made the assumption that these students would be less likely to repay debts because they would not receive high-paying jobs. When a student who had received a credit card while majoring in math was denied a card because he had changed his major to rhetoric, the practice came to the light of public scrutiny.

Privacy is especially important to students until they have gained sufficient autonomy, knowledge, and experience to make reasoned decisions about the actions they wish to take and are prepared to suffer the consequences of those actions.

Technological Advances: Privacy Challenges

Several existing or emerging technologies that have great potential for improving the way higher education serves students also have implications for their privacy rights. The discussion that follows illustrates the privacy issues that can and do arise in the context of deploying these rapidly emerging technologies, including real-life incidents that have occurred in colleges and universities. While the nature of privacy violations hasn't changed, network technology has changed the magnitude of potential damage, thus making it necessary to consider old problems in a new light.

The Internet

The Internet is a combination of international, national, state, and local electronic networks that enables people around the world to rapidly and easily access and exchange information. Internet privacy issues relate in part to the structure of the Internet itself and in part to its breadth and speed. The instantaneous and global nature of electronically networked communications magnifies simple errors. It is possible to transmit sensitive information, whether by accident or malicious intent, to a global audience in seconds, without ever being able to retrieve the information, rectify the error, or even stop its unlimited retransmission, as illustrated by the incident that follows.

> In 1994, a midwestern university student sat at a public computer to read his electronic mail, unaware that a Trojan horse program had been placed on that machine. The program, though appearing to be a normal sign-on screen, captured and stored his password. Only days later, a racially offensive and threatening e-mail message was sent over the Internet to thousands of users under his name by the person who had captured and stored his password. The racist message appeared to be coming from the student, and he became the target of thousands of angry and threatening messages in response to the racist content. Though it was later proved that the individual whose name appeared on the message did not send the message, he is still plagued by individuals who continue to find the message living in cyberspace and become outraged. The student is the focus of complaints and continued suspicion because his name has been widely associated with this racist content.

Threats to privacy on today's Internet have in part grown out of its origins. Participation in early networking activities was limited to research centers at colleges and universities and government development facilities. The original Internet was designed to facilitate the widest possible sharing of information, so the security measures essential to protect privacy were not emphasized. With access to the Internet available to the general public, and with its extremely rapid growth, there is an increasing awareness that the weak security practices inherited from the network's early culture urgently need to be addressed.

Fortunately, technologies supporting secure transmission of data over the Internet are now becoming available, and institutions of higher education are beginning to deploy them. (See the discussion below, beginning on page 10.) The effectiveness of these technologies will be limited, however, until their use is widespread and standardized. Institutions concerned about the security, privacy, and accountability of information sent over

the Internet should both install appropriate systems on their own campuses and get involved in network-wide activities to promote the standardized use of these systems throughout the Internet.

Higher education communities need to be cautious and thoughtful in the way they use the Internet, especially in implementing network-based applications that require confidential handling of student information. In addition, colleges and universities need to establish and promote institutional standards and policies to support and guide the use of networked information resources and technologies. Without such widely understood guidelines in place, privacy violations such as the one that follows can and do occur as a result of ignorance.

An economics professor at one of the Big Ten schools decided to post the final grades of his students, using their student ID numbers (Social Security number plus one digit) as identifiers, on a local Gopher server, not realizing that the information would be accessible from any place that had an Internet connection. Students were not happy with this use of technology for posting their grades and, coincidentally, their identification numbers (SSN+1) to the Internet community.

Electronic mail

Electronic mail is a technology that is almost universally desired and one upon which colleges and universities increasingly depend. If an e-mail server is down for even a brief time, the immediacy of the outcry from users illustrates the importance of the technology to most of the campus community.

The threats to privacy related to electronic mail on networked mail systems are many. The primary issue involves the nature of e-mail itself. Is e-mail more like a phone conversation (for which records are not maintained and which is considered private, with laws to protect privacy), like sealed letters (which are subject to records retention acts and policies, for which there are strong laws protecting against intrusion as well as a strong tradition of respect for its sanctity), like post cards (for which there is sanctity protected by law and tradition but which everyone understands may be seen by prying eyes), or like a bulletin board (for which there is no expectation of privacy at all)?

The law has not yet given the community definitive guidance on this issue. The answers to these questions in some ways dictate how electronic mail will be treated by the institution. Unless an encryption technology is used, e-mail is not assured of confidentiality. Once sent, it may pass through a number of intermediate systems before reaching its final destination. At any point along the journey, it has the potential for being intercepted, read, stored, modified, destroyed, or forwarded. To a degree, of course, all of these deficiencies also apply to traditional paper mail. In the world of e-mail, however, the abuses may be carried out by a much wider range of individuals, and without any telltale traces left behind.

Differences in expectations regarding ownership and handling of e-mail messages is another issue. These can arise as a result of cultural differences among users and systems managers, and/or the lack of policy defining the status of e-mail as confidential or public record, as in the following incident. Institutional policy is needed to spell out standards for handling e-mail by system administrators, technologists, and members of the community — that is, will e-mail be handled and managed as confidential?

A system manager at a university medical center, receiving complaints from male employees that a female student was using the e-mail system to solicit sex, decided to take matters into his own hands. He reasoned that as a manager he had the responsibility to see to it that the e-mail system was used appropriately, that is, for the conduct of business. Employees understood the system to be for all of their uses, social and interpersonal, though primarily for work-related uses. The manager intercepted all messages to and from the student daily and reviewed the content of those messages for evidence of wrongdoing. Once the manager's practice was reported to university officials, he was informed that his actions must be stopped as they violated good management practice, ethics, the privacy of all of those who unwittingly communicated with the woman, and possibly the law (Electronic Communications Privacy Act, 1986).

Another issue regarding e-mail occurs when it is implemented without technologies in place that will authenticate the sender and protect against forgery. In such circumstances, it may be impossible to know who the actual sender is, as in the following incidents.

Two universities have reported forged mail purporting to come from their president with the obvious confusions on the part of the recipient. At one eastern university, mail which was sent to the president, supposedly from the director of housing, announced his resignation. Before the president could be informed that the mail was a forgery, the resignation was officially accepted. At another university, a forged electronic mail message posted in the name of a professor cancelled a final examination, causing students to miss the test.

Still another issue regarding e-mail is its permanent nature. When an individual deletes a message and believes that it no longer exists — assuming that the recipient also deleted the mail and did not forward it — has the message really been deleted? Even from backups and archival copies? Policy regarding what should be preserved and saved as official correspondence and part of professional duty within institutions should be established. Such policy relates to the fair information practice of minimization, discussed on pages 15-20.

Institutions should consider the nature of e-mail when addressing what types of information are appropriate for transmission via this medium. Until more effective host and network security methods are in widespread use, the technical realities of this technology may cause it to fall short of the campus community's expectations, policies, and standards. Encryption technologies (see page 11) hold promise for ensuring the confidentiality of electronic communications, if they do not prove too cumbersome for routine use.

World Wide Web

The World Wide Web, a network of servers on the Internet that provide information and hypertext links to other documents, allows audio, video, graphical, and textual content to be transported, accessed, and exchanged worldwide. The Web has already found a role in student information services. Comments one registrar, "For enrollment management, the Web allows colleges and universities to interact with students and prospective students in a totally different way. It allows them to find out information about the college in which they are particularly interested in much more depth than a hard-copy publication."

Along with the beneficial uses of this technology come a few privacy implications for those who use it. One concern is the ability of Web browser software to "cache" (temporarily store) information that has recently been viewed. When student records are accessed via a Web interface on a public microcomputer, the next person to use that computer may be able to view previously loaded information, depending on the system design or configuration. It is also the case that the various Web locations visited by the user of a computer are cached and, as in the incident below, this cache can be viewed by anyone with access to the computer.

A residence hall administrator at one midwestern campus found that students knew little about the records their Web browsing activities automatically stored on their machines until an incident occurred. One student wishing to discredit another entered his dormitory room, accessed the Web cache on his machine, and then proceeded in public forums to announce what information the student was reading and how often he was accessing it. The student was publicly embarrassed and ridiculed.

Online monitoring and tracking by network systems (see sidebar, page 18) is usually employed to efficiently manage systems and ensure against overloads and breakdowns, but the monitoring tools may be used for other purposes, as well, some of which may constitute misuse. For example, the tools might be used to construct detailed logs of an individual's behavior — such as the network sites s/he visits or the applications s/he uses — thus creating new personal information about this individual. Even if the use is not intended to hurt specific individuals, the threat of embarrassment may have a chilling effect on their use of the system if the practice of monitoring or logging transactions is not managed to protect privacy, as in the following incident.

Twenty-eight graduate students employed as teaching assistants at an Ivy League university were shocked to discover that the campus network system permitted other users to see a list that revealed they had downloaded pornography. Apparently, the transmission of electronic mail and the transfer of files from the Internet were regularly recorded in a public log in the system, which is used throughout the university by faculty and students.

This issue is analogous to the long-standing privacy issues surrounding library circulation records, and more recently records of purchase or rental of videos. Policies regarding such logging and monitoring activities and the information maintained in such logs — information that, if personally identifiable, is part of the student record — should be in place to guide such practices.

Organizational practices involving the Web may also violate individual privacy. For example, administrators may require publication of student information on the Web that students may consider personal and wish to restrict to campus viewing. Institutions should encourage thoughtful discussion of both the positive and potential negative effects of using the Web, to help develop policy in this area.

Another concern in this context is use of the Web for the collection and transport of confidential information. College and university administrators want to be able to share information (such as testing and transcript information) easily between institutions and to gather admissions and financial aid information easily and quickly from individuals all over the world who wish to apply. The online environment holds remarkable promise for such activities, but it is important to consider privacy expectations when evaluating what information to request or disseminate via the World Wide Web, and what level of security is needed to provide what the institution deems reasonable assurance of privacy protection.

Digitized signatures

Digitized signatures are image replicas of the individual's own handwritten signature obtained during a signing operation. (The pads/signature recording devices beginning to be employed by major department stores and express delivery services are an example.) Digitized signatures should not be confused with digital signatures, one of a number of technologies that enhance security in a networked environment (see discussion about encryption, page 11). Many institutions are considering, or have implemented, procedures for collecting digitized signatures.

Some colleges ask faculty, staff, and students to provide digitized signatures to include on identification cards for confirming identification when purchases are made or checks signed. Others capture and store digitized signatures, rather than paper forms, to improve the efficiency of routine processes.

There are advantages and disadvantages to this process. The advantages are a reduction in the amount of paper and staff time needed to file, maintain, and retrieve documents that require an original signature. The downside of stored digitized signatures is that their unauthorized use would constitute a forgery with exactness never before possible. Colleges and universities electing to use this technology need to consider the security of the system and the storage medium employed, as well as the procedures for collecting the signatures.

Digitized photographs

Digitized photographs are simply that — photographs that have been converted into digital form and placed on a computer for storage and reproduction. There are many interesting uses that can be made of digitized photos. Photographic directories of classes of students can be made for faculty members, helping them to more quickly learn student names and to confirm the identity of individuals in their classes and those taking class examinations. Photographic departmental directories can be created, helping departments form communities and helping faculty, staff, and students get to know each other. Digitized photos can be electronically submitted with graduate school applications, employment applications, and letters of introduction to expedite the application process.

As illustrated in the incidents described below, however, some students consider photographs to be personal pieces of information and may wish to have them treated accordingly. Institutional issues associated with digitized photos include determining when and why images of students are required, how images of students will be stored and secured (to prevent alteration, misrepresentation, or misuse), and who may access them. Should an

administrator require individuals to place their image into "cyberspace" for access by unknown individuals? Should prospective employers have access to photos of students or others? Institutional policy should address these and other issues related to digitized photographs of students.

Incidents occurred in 1996 in which students complained because their digitized photographs were transmitted on departmental Web home pages without their informed consent. In one case, the department required all students to have their pictures taken for transmission on the Web page with no opportunity to opt out. In the second case, students believed their pictures were being taken for use within the university community only. In a third case, graduate students who were unhappy about being ordered to have their photos taken for Web display nonetheless complied because they knew the dean favored this use of technology and they were afraid to refuse. In all of these cases, the students who objected to the practice expressed discomfort because they felt more exposed and accessible to strangers, and feared for safety due to what they saw as unnecessary use of their personal image. Other students at these universities, however, have created personal home pages on which they have enthusiastically included their photos. The difference is a matter of personal choice and control.

Desktop video

Networked video at the desktop is technology that holds tremendous potential for education. This technology combines video cameras for images and sound, computers for access and delivery of information, and networks for transporting the images, sounds, and textual information. It can provide this combination to many different locations on a campus, nationally, or internationally with the speed and ease of the Internet. Combining sources of information from the computer, the Web, live video, audio recordings, and written information, creative presentations can be merged and sent over the campus network to residence halls throughout the institution. Special service announcements, event notices, special interest programming, and classroom presentations can be simultaneously transmitted across campus.

As with other technological advances, with positive opportunities for collaboration and creation also come opportunities for abuse of privacy. In addition to deliberate abuse, such as one individual observing or broadcasting another individual's behavior without his or her awareness, authorization, or consent, there is the possibility for unintentional privacy violations. As this technology becomes more common, unless new mechanisms are developed to notify users when broadcast is occurring, individuals may forget that the desktop video broadcast capabilities are turned on and discover that what they thought was a one-to-one exchange with a colleague in an office was really a broadcast discussion over the campus network.

Electronic Data Interchange

Electronic Data Interchange (EDI) is the computer-to-computer exchange of electronic information in a standardized format. The standardized formats, or transaction sets, are developed through the American National Standards Institute (ANSI). Using special software, information is retrieved from the computer, placed in the standardized format, and sent usually via a network or phone modem. The receiver takes the formatted information and filters it through special software and into the appropriate file(s) in the computer.

For years the business community has been exchanging such things as purchase orders, invoices, and inventory information. In 1992, ANSI approved a transaction set (TS 131) for a Student Educational Record, developed by the SPEEDE (Standardization of Postsecondary Education Electronic Data Exchange) task force commissioned by the American Association of Collegiate Registrars and Admissions Officers (AACRAO). Since that time a number of other education-related transaction sets have been approved, including Application for Admission, Verification of Enrollment, and Test Scores. Several hundred postsecondary institutions are currently electronically exchanging student information using SPEEDE standards. Among the many advantages are speed, elimination of data entry and data entry errors, and elimination of postage costs.

However, EDI presents a number of privacy and pro-

tection issues for institutions that exchange information electronically, especially when the exchange is transmitted via the Internet. While the business community has heretofore utilized private networks or VANs (value added networks), availability and cost have made the Internet an obvious choice for EDI for postsecondary institutions. Thus the issues facing institutions that choose to use the Internet for EDI are much the same as the issues already discussed for this transmission medium — information security (whether the information should be encrypted and at what level), authentication (how to ensure that the information received is authentic rather than fraudulently created and transmitted), authorization (how to ensure receipt by the appropriate office), and integrity (whether the information has been intercepted and altered by an unauthorized party).

Data warehouses

Data warehouses are fast becoming a standard information resource at colleges and universities, providing tremendous access to information, both in terms of volume and speed. Essentially a data warehouse is a database containing information extracted from one or more production databases. For example, a data warehouse might contain information extracted from a student records database, a human resources database, a financial database, etc. Not only does this eliminate the need for several separate requests for data, but it also provides faster and easier access to information than is typically the case when requests are made to production database administrators.

Data warehouses are often housed in a client/server environment, making information access and utility far easier than in the past. Academic and administrative units can quickly access their data for a variety of tasks ranging from running labels for their enrolled students to performing high-level decision-making and analysis. People and departments requesting access to data warehouses point out that often the information sought is owned and maintained by the requester to begin with. In fact, one of the frequently cited benefits of a data warehouse is that it often results in "cleaner" data. Information owners can easily view and utilize their data warehouse information, and they are quick to correct errors in the production database.

However, this powerful information resource also presents significant challenges related to security and proper use. Ensuring that specific information is viewed and retrieved only by the appropriate parties becomes more difficult with the amount and variety of information housed "under one roof" in the data warehouse. Ensuring that the meaning and attributes of the data are clearly understood by users is essential in order to eliminate the possibility of inaccurate or misleading analysis and decisions. Clear policies regarding what information may or may not be appropriate in the data warehouse must be established. Secure communications must be in place before users have access to data in the warehouse. This is especially true in view of the fact that most access to data warehouses is via the campus network.

Data warehouses present an exciting resource and tool for more informed decision-making and analysis, but they also present very significant challenges to proper use and access to information.

Technological Advances: Privacy Opportunities

A number of other rapidly developing technologies may hold the keys for greatly *improving* personal privacy, while facilitating access to information in a networked environment. Such "security" technologies are the essential element that will enable the types of distributed information interchange that colleges and universities seek without compromising users' fundamental privacy.

There is no single security strategy that will apply universally to all institutions and all environments. Rather, each institution will need to develop sound security strategies that integrate emerging security techniques and technologies effectively in the context of its own unique environment. Several security technologies may be effective, now or in the future, depending on the institution's specific network architecture and needs.

Firewalls

Firewalls are methods or devices that restrict access between a trusted internal network and an untrusted, or public, network. While firewalls are perhaps not as widely deployed in universities as in corporate environments because the user base is quite different (for example, not all users are employees on LANs or workstations that are assumed to be trusted), firewall technology can be used to good effect for certain areas or appli-

cations. For example, firewall technology may be applied for administrative or medical networks, or at either the main Internet interface or the college or departmental level.

Encryption/digital signatures

Encryption is basically "scrambling" some or all data in ways that are computationally secure, turning plain text into cipher text. Encryption is fundamental to protecting the confidentiality and integrity of personally identifiable information when it is being transmitted through untrusted or public networks because of the ease with which unencrypted data can be intercepted, rerouted, or modified while en route. Two common methods of encryption are public-key encryption and private or secret-key encryption.

In public-key encryption, there is an element of the encryption process that can be known by all — the user or service's public key. There is also an element that is private and cannot be shared — the user or service's secret key. If one, for example, wishes to send an encrypted message to someone, s/he encrypts the message using the recipient's public key, but the recipient can only decrypt the message using the secret key known only to him or her. Public-key technology is frequently associated with digital-signature technology since the user can "sign" a piece of correspondence with his or her secret key and the validity of the signature (and hence integrity and source of the correspondence) can be verified by the recipient with just the public key of the sender. An example of public-key encryption technology is Pretty Good Privacy (PGP).

Private or secret-key technology relies upon a shared secret. If something is encrypted with a particular secret key and transmitted, only a user or service that knows or holds the same secret key can decrypt the message.

Today, secure Web server technology and other applications are making use of cryptography to verify "digital certificates" associated with various clients, servers, or users. A digital certificate is a statement about the identity of an object (for example, a person or service) signed by an independent and trusted third party. A certificate generally contains three elements: subject name and attribute information, which describes the object being certified (perhaps the individual's name, e-mail address, or work unit); public-key information, which provides the public key of the object being certified; and finally the Certifying Authority (CA) signature. The CA cryptographically signs the attribute and public key information. Those receiving the certificate can check the signature and accept the attribute and public key information if they trust the particular CA.
S/MIME, a method for secure electronic mail that will be employed in most standard browser software, relies on digital certificate technology. There are a number of complex issues surrounding establishment of a certificate authority hierarchy with which institutions will need to become familiar and address in their planning processes in the near future.

Employing authentication technology will help to prevent incidents like the following from occurring.

> The 13-year-old daughter of a hospital records clerk in Florida used her mother's computer on an office visit to print out names and addresses of patients treated at the emergency room, and then, according to police, went home and telephoned seven of them to tell them falsely that they were infected with the HIV virus. Upon her arrest, the girl told police that this was just a prank. One person attempted suicide after the call, and all of the victims were severely upset.

Middleware technology

Kerberos is a protocol developed at MIT that facilitates trusted third-party authentication. In other words, users and services are authenticated to one another based on essentially a mutual "introduction" by a source that both trust — the Kerberos server. The protocol makes extensive use of encrypted tickets for services, and user passwords are never sent across the network, even in encrypted form — they are only entered at the individual user's workstation. Kerberos uses the secret-key encryption methodology which relies on a secret shared between principles (for example, users or servers) and the Kerberos server.

The Distributed Computing Environment (DCE) is a collection of middleware services that expands upon Kerberos capabilities (which are limited primarily to authentication). DCE Security Services include authentication, authorization, and privacy (encryption) options.

Thus,using DCE it is possible not only to mutually authenticate users and services but to establish granular control over what a user will be able to see or modify.

There are a number of shortcomings with both Kerberos and DCE, but they do address some of the more complex problems with network-related security in large-scale, heterogeneous environments.

Some institutions are forming partnerships to work toward solutions using these technology environments, such as the members of the Committee on Institutional Cooperation (CIC), the academic equivalent of the Big Ten athletic conference. CIC universities are working with the Open Software Foundation to develop a Web-based authentication and authorization mechanism that maps any institutional security realm to a DCE security environment which in turn provides for the encrypted transmission of information across the Internet. The goal is to allow users to make use of a Web browser of choice to move information across the Internet encrypted from end to end. This Web client will be used first to allow faculty, staff, and students at one institution to access licensed material stored on a server at another institution. The second application will be for the creation of a buying consortium among CIC institutions, so that faculty and staff can order materials from an electronic catalog and arrange payment via corporate credit cards. One can imagine the future use of the secure Web client for the transmission of student information from one institution to another across the Internet.

Token cards, smart cards, and one-time passwords

Token cards, smart cards, and one-time passwords are designed to help overcome the vulnerabilities associated with reusable passwords. With a token or smart card, authentication to a computer or network resource is based not only on "something you know" (a user ID and password), but also "something you have," the card itself. Tokens may operate in various ways, for example by calculating a response to a challenge issued by the server, or by providing a unique time-based number that the user furnishes to the server. A smart card may contain various items of information that are unique to the user that can be used in the authentication process. The primary necessity is that the authentication sequence cannot be completed unless the user is in physical possession of the card, and the exact information the card holder supplies during authentication is not repeated in subsequent sessions. Therefore, "sniffing" (capturing) the information does not allow the intruder access to the service at some later date. One-time passwords are based on the same basic philosophy — that authentication must be unique each time. But they may not require a hardware device. An example of a one-time password implementation is S/Key.

Biometrics

Biometric technology, such as voice recognition, fingerprint matching, or hand geometry can be used to authenticate the user based not on something he knows or something he has, but rather by a physical characteristic that cannot be changed. While biometric technology is still relatively expensive, as it becomes less costly and more computing power is available to support it, biometric authentication may become practical for some college or university environments or applications.

These technologies illustrate that it is possible to resolve many current security-related privacy concerns, but it will take creative, well-planned, integrated application of security technology to do so. Colleges and universities should begin planning for the future security architecture in order to enable both open *and* secure applications. It need not be an either/or decision.

Balancing Technology Benefits and Threats to Privacy

Prior to implementing new technologies, colleges and universities should carefully explore both their potential misuses as well as the opportunities they afford, balancing the individual right of privacy against the benefits to the institution in each application. Colleges and universities do not make decisions about using such widespread technologies as e-mail and the World Wide Web in a vacuum; they function in a world where many other players and external forces — government, private sector, and public demand — influence the ways in which they apply technology. The external environment also shapes what is considered an "acceptable risk" and this will differ from campus to campus. Some tradeoffs may need to be made in creating institutional policy, tradeoffs that only a broad set of campus stakeholders working together can best determine.

As institutions redefine how they process, store, display, and disseminate student information and student-generated information, they will also confront potential individual student desires for limiting release of specific information about themselves through electronic networks. In responding to rapid technological change, consideration must be given to the effects of such change on the concept of consent. Twenty years ago, students gave consent for private information to be collected and released by the institution with the understanding that the information would be kept on cards or microfiche and only accessed manually by authorized personnel. Today, the same information is often available in relational databases, retrievable instantly over electronic networks and on individual machines that might have their electronic locks tested by anyone in the networked environment. Thus the basis for consent may change based on technological innovation alone.

Used to its full potential, technology can empower both ends of the spectrum — those students who desire to control the electronic release of any information about themselves and those who see positive advantage in releasing most, if not all, personally identifiable information. The challenge for information technologists is not just to provide access, but to do so within the parameters of a well-defined institutional policy on privacy and information access. Where a new technology introduces a privacy concern, the tradeoff between ease of use and ability to keep information confidential should be clarified and decided where possible with input from the people affected.

In summary, colleges and universities have a responsibility to purposefully reexamine and define their values and institutional needs with respect to the implementation of new technologies and their impact on privacy; to employ fair information practice that reflects those values and needs; and to make decisions about technology deployment within this framework. The next section explores fair information practice, especially in the context of networked information environments.

IV. Principles of Fair Information Practice and Policy

Policies on privacy and the handling of student information in networked environments should rest on a firm foundation of principles of fair information practice. Such policies play a significant role in promoting coherence across the institution by providing clear rules and procedures for student information management.

While much of the legal foundation of such policies is derived from FERPA, the ethical foundation is derived from the values of the college or university. The process of creating policies often requires a reexamination of these values, to reaffirm or clarify them, and that exercise may uncover strong feelings in the academic community. Thus all stakeholders need to be involved — student services and other administrators, faculty, students, staff, legal counsel, and technology professionals. (See pages 34-37 for examples of policy-building strategies and processes.)

This section outlines eight relevant principles of fair information practice that our task force believes provide a framework for evaluating campus values and creating policy with respect to privacy and access to information in a networked environment:

- ✓ Notification
- ✓ Minimization
- ✓ Secondary Use
- ✓ Nondisclosure and Consent
- ✓ Need to Know
- ✓ Data Accuracy, Inspection, and Review
- ✓ Information Security, Integrity, and Accountability
- ✓ Education

These principles, though variously titled in the literature, have been recognized over years of legislative intent, action, and implementation as the foundation for sound information practice. Documents such as the *IITF Principles for Providing and Using Personal Information* and

European Directive on the Protection of Personal Data have been useful resources (see Appendix H for others).

To aid policy development in the academic community, this section provides a definition of each principle, notes relevant law and its implications for practice, and provides examples of practices that illustrate lesser and greater application of the principle. A variety of issues are identified, especially those that arise in a networked environment, that institutions need to address in establishing policy or procedures.

The Principle of Notification

1. Definition

The notification principle provides that students be informed of *what* information is being collected; *who* is collecting the information and *from whom* it is being collected; *why* the information is being collected (i.e., the intended use); *what steps* are being taken to protect the confidentiality, integrity, and quality of the information; the *consequences* of withholding information or of providing false or incomplete information; and any *rights of redres*s, such as inspection or challenge. These elements of the notification principle provide the basis for knowledgeable actions when individuals are asked to give consent for others to have access to their information. Without solid knowledge, consent can be hollow instead of informed. This is what is meant by informed consent.

Notifying students of the gathering, storing, and responsible management of information is essentially an awareness activity. In their rush to complete admission, orientation, registration, and financial aid paper work, students may be unaware that data are being collected about them. As a result, they may not take time to consider or question staff about such issues as disclosure or use of their data. If students are notified of where the information is being stored and under whose authority it is being collected and managed, they will have the opportunity, at a later date, to check on the accuracy of the information and provide updated information when appropriate to the collecting office.

Note that the notification principle applies to information collected both from and about the student. The means of notification will be different in these two cases, but the principle remains the same.

2. Relevant Law

FERPA requires each institution to inform students annually of their rights of privacy and access under the law and to give public notice of the categories it has designated as "directory information," that is, certain information about students (such as name and address) that may be made public without consent unless the student objects.

3. Policy Issues

Within the electronic environments of colleges and universities, notifying and informing students is a process that may become increasingly problematic. In such environments, information is being stored and transported between many different offices, on a continual basis. Questions concerning notification frequency, intensity, and granularity and scope will need to be addressed in building policy about handling student information in this environment.

Frequency

An institution must notify students annually of their privacy rights under FERPA. Many institutions publish such notifications in registration materials. But this may no longer be adequate in a world of dynamic technology, where new databases, information paths, and security systems are being created, modified, and recreated continuously. This same dynamic technology can be used to automate and facilitate the notification process; for example, e-mail messages and the Web could be used to deliver such information.

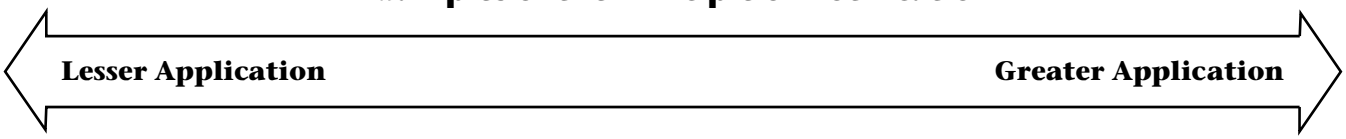
Intensity

How active will the institution be in ensuring that students have received and understood their notifications? Is a fine-print footnote on a registration form adequate, or should each student receive a personalized letter? Should students be required to positively acknowledge — by signature or other means — receipt of this information?

Granularity and Scope

With the increasing demise of host-based computing, student records are often no longer housed in and controlled by a single central system. In a distributed computing environment, to what extent should students be notified of each record's distinct usage, security, and

Examples of the Principle of Notification



- ☆ The institution provides annual notification information in the student handbook. That notification includes information about students' rights to privacy and about what information the institution has identified as directory information.
- ☆ Students are not informed that data are being collected as a function of system transactions.
- ★ Students are notified and informed each time personal information is collected and told the purpose for which it is being collected.
- ★ Students are notified of the office under whose authority their information is being managed and maintained, as well as any secondary offices to which the information might be distributed.
- ★ Students are informed of the existence of any personally identifiable system transaction data.

other characteristics? How much detail is it reasonable to provide before the volume itself becomes an impediment to true understanding?

4. Task Force Recommendations for Notification

◆ Institutions should notify students of their privacy rights with the same prominence and frequency afforded other important areas of campus life, such as residence-hall regulations, course descriptions, and meal-plan options. A useful comparison may be made between notification of campus judicial system regulations, which focus on student responsibilities and punishment, and notification of privacy policies about student records, which focus on student rights and abilities.

◆ The institutional approach to notification should also take into account the technological sophistication of the student body. This and other local considerations should be applied in order to provide useful and meaningful information to students. An effort should be made to avoid overwhelming detail on the one hand and overly vague generalities on the other.

◆ When formulating policies and procedures concerning student notification, campuses should consider the effects of the distribution of databases to non-centrally controlled systems, as well as transaction and tracking data maintained as a by-product of daily operations. Policy should determine how students can be informed of the existence of such databases and systems.

The Principle of Minimization

1. Definition

The principle of minimization relates to what kind and how much information is collected from students, with an emphasis on gathering the minimum amount of relevant personal student information needed to accomplish a legitimate, identified institutional purpose. Associated with this principle is the responsibility to delete information when it is no longer needed. The challenge is for an institution to identify those elements that are truly the "minimum" needed, avoiding collection for collection's sake or for "potential future use."

2. Relevant Law

A number of laws proscribe collection of certain information. The federal Privacy Act requires that agencies of state and local government not deny a benefit to an individual for failing to provide a Social Security number unless prior to 1974 there was a law or regulation authorizing such a demand. A few state laws prohibit private and public institutions from asking applicants about arrest records or about certain sealed criminal records; in other states an applicant may legally deny the existence of certain criminal records about himself or herself. The federal Fair Credit Reporting Act prohibits the use of credit reports for admissions or for internal

investigations. Federal law and state laws prohibit intercepting telephone, modem, electronic mail, voice mail, digital, or fax communications without consent of at least one party to the conversation, unless an institution is monitoring for "the protection of [its] rights or property." Some states require the consent of both parties.

3. Policy Issues

One driving force for increased collection of information in higher education is the requirement by state and federal agencies for the reporting of increasing amounts of student data. Some of that data may be information the institution would not otherwise need for its purposes: ethnicity, for example. In some southern states, laws have recently been passed which require institutions to collect and use more, rather than less, personal student information.

From a purely management point of view, what information collection philosophy is practical and efficient? The institution's information management strategy will to some degree guide its data collection policy. Recent demands to cut costs in higher education may inspire more streamlined information management, prompting institutions to ask, "Do we really need to collect this information? Can we eliminate this questionnaire? Do we need to retain this information as long as we have in the past?" In the new interactive, online environment, administrators can search for ways to reduce or eliminate altogether some of their massive databases of personal information. Are there ways that the information can be retrieved later from other sources on an "as-needed" basis? Can a student be asked to provide an electronic source for locating information about him or her, rather than provide the information itself?

Other policy issues related to minimization include the automatic collection of data by systems, appropriate sources of information about students, collection of sensitive data, collection of data for emergencies, and how long data should be kept.

Transactional Data Collection

The nature of information technology is such that inexpensive, widespread collection of information is increasingly possible. As more of the day-to-day operations of the college and university are automated, an enormous amount of transactional information is automatically generated, quantitatively dwarfing the traditional structured databases of relatively static information. As students move around campus — physically and virtually — and interact with departments and service providers, they inevitably leave behind traces of their activities. A student who walks into a computer lab, logs onto the network, browses the bookstore's Web server, orders a text, and enters a credit card number for payment may have created a dozen distinct records in an equal number of databases and logs, each under the administrative control of a separate institutional unit.

Information may be gathered as a function of the commercial product or public domain software used by the institution, rather than as a deliberate institutional choice. Should information be collected and retained merely because the hardware or software permits it?

Appropriate Sources

Should the only source of information about students be the students themselves? Proponents of this view assert that if the student has not provided the information directly, its collection is inappropriate. However, in a campus context, as in many other social venues, this is overly simplistic. Certain elements of information that are not provided by student forms, questionnaires, or admissions materials alone may be mission-essential — for example, grades provided by faculty. There is also a genuine institutional need for the collection of information generated by some real-time student actions — logs of debits against a meal card are needed to ensure correct balances, and the number of printed pages generated by a student in a public computer lab is needed for billing purposes. Such logs are not strictly "provided" by the student but are created as the result of student action. Campus debate will likely center around the issue of balance in data collection.

Sensitivity of the Data

Another issue in the debate regarding the minimum data set that should be collected about students is the sensitivity of the data themselves. Some argue that the more sensitive the information, the less it should be collected. Others argue that institutional need, not sensitivity, should dictate the information collected.

Advocates of the first viewpoint have suggested that no information should be collected about the exercise of First Amendment rights — freedom of assembly, religion, speech. There are times, however, when institutions may

Examples of the Principle of Minimization

Lesser Application ⟷ **Greater Application**

- ☆ The institution places few restrictions on the type or amount of data collected, and uses multiple sources to collect information about students.
- ☆ Data are monitored, tracked, and maintained based on defaults built into network software rather than conscious decisions about data collection.
- ☆ The institution collects a range of contingency data because of concerns about institutional liability, and also for potential use.
- ★ The institution collects only the information that is necessary to conduct specified institutional business. The more sensitive the data, the more closely the institution adheres to this practice.
- ★ To the greatest extent possible the source of information about students is students themselves.
- ★ The institution has adopted the practice of having an associated disposal schedule for every element of personal information that is collected.

need to record religious affiliation. For example, students may need to provide religious affiliation in order to be assigned a chaplain. Also, student activity offices may unavoidably gather information about political affiliation from information about membership in campus clubs. External relation offices of colleges and universities may inadvertently gather information about both religious and political affiliation as a result of news clips, videos, or other media development activities.

Financial aid information has always been considered sensitive information, yet its collection is obviously essential. Other areas are decidedly more gray, however. For example, as part of the admissions process, should the institution collect arrest or conviction information? What kinds of data *are* appropriate to collect as part of the admissions process? The following practice illustrates the potential for increased collection of sensitive data by some institutions.

> Under new admissions guidelines effective in 1998, one West Coast university admissions office plans to admit up to half an incoming class on "special circumstances" instead of considering race or sex. This will require applicants to submit information about difficult family situations, economic disadvantages (such as data about one's neighborhood, financial status, parents' educational level and layoffs), psychological difficulties, and so forth.

Collection of a student's Social Security number is another issue (see sidebar, page 19, for a more detailed discussion). As the example below illustrates, however, it is sometimes difficult for an institution to elect not to collect the Social Security number of students.

> One admissions officer would like to move her university's student data systems away from using the Social Security number as the key to the database, supporting the notion of using a unique student ID number instead. However, the state in which the university is located requires the collection and reporting of information using the Social Security number as the common identifier — a major obstacle toward the university's changing this practice. Such conflicts are not uncommon.

Emergency Data

Should the institution collect information it would only need if an emergency arose, risking that the same information later may be used inappropriately? Two examples will help clarify this issue. Should a campus with a low crime rate collect and store information about all entry to locked buildings if the need for this information might only arise if a robbery or other crime occurs? Should the computer center collect and store enough information to be able to retrace the steps of any and all possible computer crimes?

In many ways, the safest philosophical approach regarding the principle of minimization is "no data, no dilemmas." However, from a practical perspective, some level of contingency or emergency information is an essential part of an institution's operation. The issue, again, is one of balancing privacy with the institution's need to protect itself against potential liability.

Archiving Issues

How long should data be kept and under what conditions? When are the purposes for which the information was collected deemed to no longer exist? Legal restrictions preventing disposal need to be factored into these decisions. In a networked environment, issues include the existence of system backups and archives and coordination of data disposal from all such file space, including e-mail messages.

4. Task Force Recommendations for Minimization

◆ Colleges and universities should gather all legally required student information and the minimal amount of additional information to accomplish a legitimate

ONLINE MONITORING AND TRACKING

Online monitoring and logging — watching and/or recording activity on a computer or network — is necessary to manage the flow of traffic over certain systems and to trace incidents of misuse of those systems. However, this practice can itself be misused in ways that result in a violation of the privacy of individuals.

On some machines there are public routines that, when monitored and analyzed over time, can provide a lot of information about the computing habits and practices of a targeted individual. One may be able to tell the hours during which the person uses particular machines, the amount of time spent doing electronic mail, or even the site at which the person is working. With enough time and persistence, such information may be combined with other publicly available information. If such data begin to be used to draw conclusions about the nature of an individual's use, the people with whom s/he communicates, the amount of time an individual accesses certain content, or the nature of their affiliations on the network, the privacy of that individual may be seriously violated.

It is also possible to write a basic program specifically to scan for particular user IDs or unique names, gathering information each and every time that user signs on to a service on the network. In some cases such sign-on information might be routinely gathered by system administrators, for the purpose of managing the system, without violating the privacy boundaries of individual users.

Commercial service providers have already begun to capture increasing amounts of information gathered from online monitoring and logging mechanisms, using such information to develop interest profiles of the individuals accessing different sites on the World Wide Web. They then distribute such information to others who may profit from contacting individuals with particular interests. Such treatment of personal information as a commodity to be traded and sold may be a violation of the privacy of individuals, especially if individuals are not aware of the collection of such data, which is often the case.

Higher education institutions will likely begin to increase the amount and kinds of logging and monitoring procedures they use within the next few years as they tighten security on their systems and try to manage and perhaps charge fees for the ever increasing use of key services. They will need to determine what online information is necessary to effectively do the job of managing the resources, and to consider when information collection goes beyond management needs and becomes an intrusion into individual privacy. They should consider standards and policies to guide the collection, storage, release, and use of any such logging or monitoring of information that can be tied directly to an individual. And they will also need to clarify their values regarding the sale and/or release of such information for secondary uses.

NUMERICAL IDENTIFIERS

Colleges and universities should be extremely cautious about collecting, using, and disclosing Social Security numbers (SSNs) of students. There are many reasons for this:

1. Stolen or misappropriated Social Security numbers lead to thousands of cases of "theft-of- identity" or "credit theft" each month, in addition to misuse by immigrants without documentation. If lists of persons' Social Security numbers are available, even within campus offices, employees can deliberately misuse them or inadvertently disclose them or make them accessible.

2. With someone else's SSN, a stranger can impersonate that person over the telephone, in person, or online and retrieve personal information about the individual. The Internal Revenue Service, for instance, will disclose detailed tax information to anyone who provides a Social Security number of an individual taxpayer. Many banks will also.

3. The number is not totally anonymous — strangers can tell in what state it was issued and approximately what year. If grades were to be posted by Social Security number, for instance (a practice not allowed under FERPA unless permission has been given by students), a class member may be able to identify out-of-state students or older, nontraditional students, or when arranged alphabetically by name, the actual person.

4. The incidents of inaccurate SSNs are so numerous that any record linkage based on the SSNs will be flawed.

5. Many individuals have a sincerely held religious or philosophical objection to being enumerated.

6. Long after a student has graduated, the Social Security number may show up on alumni mailing labels, thus publicly displaying the numbers and exposing alumni to the threat of fraudulent use.

All of these dangers arise when a college or university uses the SSN as the student ID number. Even though institutions may need to record Social Security numbers when students happen also to be employed by the institution or receive certain financial aid, the number should be collected at the time of these transactions with student consent. These uses should not be reasons for requiring SSNs of all students.

With today's database technology, the SSN and other personal identifiers are less necessary than in the past. A search for information on Winston Smith, for instance, when all you have is first name, last name, and home address, telephone number, or date of birth, is a reasonable search today. In the past such a search would have required more computing resources than were available at reasonable cost.

When Social Security numbers must be kept on students in a college or university system, the numbers can be encrypted so that they may be used for linkage of data files, as necessary, without revealing the actual digits of the SSNs. The resulting "record linkage number" will not permit a stranger to derive the SSN even if the linkage number becomes publicly known.[2]

Still another alternative, if a campus office must have a numerical identifier to make an accurate match of a record or to detect duplicates, is to ask a student for only the last four digits of his or her SSN. This maintains the anonymity and the confidentiality of the complete number, but will be adequate for establishing matches.

An institution can avoid most of the dangers of keeping Social Security numbers by establishing its own unique student identifying number. This will require extra effort by some systems administrators. One argument against this has been that most people don't remember a unique identifier, but many studies show that a sizable percentage of people provide incorrect Social Security numbers when asked — either in error or in order to maintain their privacy. Records have a higher accuracy rate when applicants are asked to consult a document, or use an electronic device when providing an ID number, rather than to rely on memory.

In any event, the Social Security number is not a reliable means for establishing personal identity because it has been so readily available and has been subject to widespread use by impostors. Administrators should rely, instead, on what has always been the best means of establishing personal identity — personal recognition. Where this is not practical or possible, there are adequate surrogate methods, like signature comparison, passwords, personal identifying numbers (PINs) known only to the individual, encryption for authentication, identity documents with photographs, fingerprint comparison (where there is no stigma or compulsion), and forms of biometrics.

---

[2] See Eleanor Marx, "Encrypting Personal Identifiers," *HSR: HEALTH SERVICES RESEARCH* 29:2 (June 1994).

institutional purpose, avoiding gathering nonessential information simply because of the ease of collection or correlation in networked environments. Policy and practice should address means to ensure that collection of personally identifiable information has been appropriately authorized.

.

◆ Campuses should formulate a process for determining necessary log elements and log retention requirements, particularly for logs where the inclusion of personally identifiable information is unavoidable.

◆ For those log elements over which the institution exercises control (rather than those that are a default of the operating system or vendor-supplied software), designers should consider the principle of minimization and identify those elements that would really be necessary in the event of foreseeable contingencies. Those elements rather than the superset of all possible elements should be collected.

The Principle of Secondary Use

1. Definition

The premise of this principle is that when personal information is gathered from a student, it should be used only for the purpose for which it was collected (even within the same institution or office), or for a use compatible with that purpose, unless the individual has given additional consent. Thus the principle of secondary use goes hand in hand with the principles of notification, minimization, and nondisclosure and consent. Application of this principle means that an institution must articulate, when gathering personal data, precisely the purpose for which it is being gathered. In this process, an institution may discover that it has no clear purpose for requiring certain personal information.

2. Relevant Law

FERPA requires that any third party receiving personal information about a student may not permit another party to have access to it without written consent of the student. In addition, if a student waives his or her right of access to letters of recommendation, the recommendations may be used "solely for the purpose for which they were specifically intended." The intent of FERPA has consistently been that information collected for one purpose not be reused without explicit consent of the individual to whom the information refers or unless the reuse is a routine use, defined as a use which is compatible with the purpose for which the information was collected.

2. Policy Issues

The principle of secondary use is one of the most critical to be examined and understood as colleges and universities network information technologies within their campus communities. Once information is gathered and stored in a medium that facilitates its fast access, sorting, transport, and reuse, this information becomes much more accessible to the exercise of new options and opportunities. Data mining and sorting information in new ways to answer new questions or to form new hypotheses is not only possible, but may seem essential as institutions seek to better serve students or more aggressively market to new students. Matching one database with another enables looking at information in new ways, perhaps gleaning new information from these combinations. Care needs to be taken that any such manipulation of data does not disclose or make accessible individual, personally identifiable data.

The integrity of institutional communications and relationships with students is established at the first point of contact, that is, during the admissions process. When an institution asks a student for personal information as part of this process, it does so within an unequal power relationship — the implication is that the student must provide the information to be admitted to the institution, and that the information is for admissions purposes. Individuals release information during the admissions process that is of varying degrees of sensitivity to them. The institution cannot know the degree to which that information needs to be maintained as private or handled confidentially.

For the sake of speed or efficiency, institutions might engage in secondary use of student data without permission. But would the individual give permission if s/he knew how the data were being used? Uses that go beyond a reasonable notion of compatibility with the original purpose might include the sale of student mailing lists by an institution to generate a revenue stream — a practice that might tempt some campuses in times of fiscal constraint. Institutions must make decisions about how to handle such things as commercial requests

Examples of the Principle of Secondary Use

Lesser Application ⟷ **Greater Application**

- ☆ The institution does not specify potential secondary uses of data at the time information is being collected, that is, agreements with students are "implicit."
- ☆ The institution broadly interprets "routine" and "related" uses of information and thus frequently uses individual data for secondary purposes.
- ★ Use of student data is restricted to the purpose for which it was originally collected; that purpose is known and explicitly articulated at the time of collection.
- ★ Potential related uses of information are defined at the time of collection or require additional consent.

for student information for marketing purposes.

The law allows for, and most reasonable individuals would agree to, routine secondary uses that are compatible with the purposes for which the information was collected. But if the institution is planning to use personally identifiable student data for non-routine purposes, the secondary use principle requires that the student be so informed and that consent be obtained.

4. Task Force Recommendations for Secondary Use

◆ The institution should be explicit about the purpose for which information is gathered at the time of its collection, and identify the routine and compatible uses of the data it expects to employ in the course of official business.

◆ Secondary uses, not included in those stated as routine and compatible, should be avoided, but where such secondary uses are deemed significantly important to the institution, policy should consider how additional permissions will be obtained from affected students.

The Principle of Nondisclosure and Consent

1. Definition

Nondisclosure means the keeping of personally identifiable information about students from third parties, that is, parties external to the college or university. The release of such information *within* the institution is addressed in the discussions of the principles of need to know and secondary use.

2. Relevant Law

FERPA forbids institutions to disclose student information without written consent, except for certain specific parties for certain specific purposes and except for directory information, which may be disclosed unless the student objects. At least eight states restrict disclosure of medical information without consent. Some states restrict disclosure of information about patrons of tax-supported libraries; a few of these laws cover private libraries.

3. Policy Issues

Policy issues related to this principle revolve around consent strategies and data sensitivity, the nondisclosure of information created by use of information resources (such as library circulation records), and flexibility of campus information systems.

Consent Strategies and Data Sensitivity

The consent strategies an institution selects will depend on the sensitivity of the data as defined by the institution's policies. Such policies should address the relative degrees of sensitivity associated with student information. For example, items that might be considered very sensitive include medical records, financial information, sexual orientation, grades, and most aspects of family history. Examples of items that might be

considered personal but less sensitive include permanent address and family size. Information that is less sensitive and whose public release would be relatively harmless might include such items as name, address, major, dates of attendance, and so forth. Data in the first two categories are usually defined by institutions as non-directory information, while data in the latter are usually considered directory information.[3]

Methods for obtaining consent for disclosure of student information include "opt-out" and "opt-in" approaches. With the "opt-out" method, commonly used for directory information, information is routinely released unless the student initiates an action to have the institution withhold the information. With the "opt-in" method, used for non-directory information, the institution withholds information unless the student has provided written consent for its release. Such consent might be required for each instance of disclosure or might be obtained on a "blanket" basis. In the former case, students might be required to knowingly consent in writing to each instance in which non-directory information is released. With the blanket consent method, students might be asked annually whether they agree to the release of non-directory information to third parties, and if they consent to such disclosure no further consent would be required for the institution to release such information. However, if blanket consent is used, FERPA requires that it must specify the party or class of parties to whom disclosure may be made (for example, potential employers) and state the purpose of the disclosure.

In an electronic networked environment, have the scope and concept of the principle of disclosure and consent changed? For example, though a student may not have objected to the public release of his or her directory information when it was to appear in a campus print directory, might the student feel differently if the institution's practice is to incorporate such information into a directory accessible on the Internet? What other kinds of information being captured about a student might s/he wish to exercise some control over? For example, the technology now makes it possible to create lists of those who belong to particular electronic discussion groups and to use that information for new purposes. While belonging to an electronic discussion group may be information a student doesn't mind another on campus knowing, s/he might object to such information being available beyond the campus. Institutions will need to develop policy with respect to whether they will publish directory information only in print or, if they plan to publish it electronically, whether it will be available only on a campus intranet or more widely distributed on the Internet, and whether consent strategies should be adjusted accordingly.

Flexible Policy, Procedures, and Systems

Given that there are likely broad individual differences in what types of personal information students feel are sensitive in a networked environment, how flexible do institutional policies, procedures, and systems need to be in enabling students to change categories in which the institution has placed a particular kind of information? For example, if disclosure of campus street or e-mail address on the Internet is unacceptable to an individual, should a means exist for him or her to place those elements in a more restricted disclosure category?

To what extent should campus systems be able to accommodate individual privacy desires? An institution's application of technology or systems design can hinder an individual's desire to exercise more control over release of information, but technology may also offer solutions that could *facilitate* a student's ability to choose. Advances in technology may make it possible for students not to have to make all-or-none decisions about the handling of their personal data. An institution's policy concerning how flexible it wants to be with respect to student choice will influence systems goals and design considerations and assignment of resources to accomplish those goals. Systems designed to provide flexibility and choice might be viewed as highly desirable and service oriented by prospective students, possibly justifying the additional costs of developing such systems. A cost/benefit analysis can help inform institutional strategy in addressing these issues.

[3] Every institution must define by policy what it considers directory information and inform students of this policy. Directory information may include such student information as the student's name, address, telephone number, e-mail address, date and place of birth, major fields of study, participation in officially recognized activities and sports (including weight and height of athletic team members), photograph, dates of attendance, degrees and awards received, most recent educational institution attended, and other similar information that would not generally be considered an invasion of privacy or harmful to the student if disclosed.

Examples of the Principle of Nondisclosure and Consent

Lesser Application ⟷ **Greater Application**

- ☆ The institution uses an "opt-out" strategy for directory information and blanket consent strategy for more sensitive information in releasing such information to third parties.
- ☆ For such data as library circulation records, the institution complies with state laws regarding privacy, but may not extend privacy to network resources accessed.
- ☆ Default positions built into campus technology applications do not facilitate individual choice in controlling personal information.
- ★ Whenever possible, the institution requires a signed consent form for individual instances of release of student information to third parties, and discourages such disclosures.
- ★ The institution develops a robust set of policies to protect confidentiality of library records and the use of electronic information resources, including use of information on publicly accessible workstations.
- ★ Campus systems are designed when possible to accommodate individual requests for withholding selective information from different communities.

Disclosure of Information Created by Use of Information Resources

There are many similarities between library records and the student records generated by the activities of student services offices (registration, admission, financial aid). By the same token, is information about which Web sites a student accesses and what information the student downloads from those sites similar to information about what library books a student checks out?

The American Library Association advises that all libraries formally adopt a policy that specifically recognizes the confidentiality of its circulation records and other records identifying the names of library users. The definition of circulation record varies from strict interpretation of items checked out through an institution's library circulation system to any information about the use of any library information resources in any format.

Of more complexity is the relationship of current laws and practices to the use of electronic resources at workstations made available at the institution. Is it an invasion of a student's privacy, for example, for a reference librarian to glance at the screen of a workstation as s/he walks by and/or to stop to suggest more effective search techniques? Should the records of what a student has accessed on the World Wide Web enjoy the same privacy protection as library circulation records?

4. Task Force Recommendations for Nondisclosure and Consent

◆ During policy development, institutions should consider defining categories of information as to their sensitivity, determining under which strata elements of information fall, and establishing congruent consent/disclosure mechanisms for each type of information.

◆ In developing policy with regard to data categorization, institutions should consider the means for students to change the categorization of an element and to specify that it be treated as more sensitive than generic policy would normally dictate. The use of technology to facilitate individual choice in this area should be considered.

◆ Consent should be specific with regard to the manner and type of disclosure, as well as the identity of the recipients and their intended use of the information. The means by which students may revoke consent should be addressed during the policy development process.

◆ The institution should ensure that students fully understand what their rights are with regard to requesting that information not be disclosed.

The Principle of Need to Know

1. Definition

This principle is based on the premise that an individual within the institution seeking access to personally identifiable student information is granted such access if and only if s/he has a need to know the information as part of an official and legitimate educational interest and in conformity with disclosure agreements. Under this principle, access to student information is based on normal job duties and the purpose and scope of the proposed use of the information.

2. Relevant Law

FERPA permits disclosure of student records within an institution to officials who have been determined by the institution "to have a legitimate educational interest."[4] State laws may add more obligations for confidentiality. Some state freedom-of-information laws require state agencies, including state universities, to release certain documents, but this release is subject to the confidentiality provisions of federal law.

3. Policy Issues

Colleges and universities must establish their own criteria, according to their own procedures and requirements, for determining when campus officials have a legitimate educational interest in a student's education records. To this end, institutions usually establish a policy that specifies who should be given access to student records and for what purpose. Such a policy generally recognizes two types of access: (1) access that is a normal expectation for the routine performance of a given job, and (2) access that is required for special circumstances.

Most such policies also address the data "stewardship" function for student information. The responsibilities of the data steward generally include ensuring that access to the information is controlled by and consistent with both the needs of the institution and the privacy needs of individual students.

With respect to job-related access, an institution's policy generally reflects its unique culture and environment. It is usually clear who needs access to student records to perform their jobs — faculty members, student services personnel, financial aid personnel, bursar's office personnel, and so forth. In the case of access requested for special circumstances, evaluating the purpose and scope of the proposed use of information can help the data steward solidify whether there is sufficient need to allow access to particular student records.

In a networked environment, institutions increasingly encounter situations that are less well defined and where effective "control" may be difficult to enforce. For example, the counseling office may think it appropriate to access computer or network access logs for students who have been identified as being at risk of failing, based on their grades. In this case, who is responsible for determining whether access can be granted to log information that is not part of the structured data in the office of the data steward? On what basis is such a determination made? What happens if the system manager and/or data steward disagree with the counseling office's need to access this information? Access to information in structured databases may also become more of an issue. As technology makes access to such databases more readily available, battles on campus over who has legitimate educational interest will proliferate.

Institutions need to consider the age of their data access policies and the potential need to reevaluate them in light of a ubiquitous networked information environment. One way to approach this challenge is to create a process that brings together a wide range of campus constituents to systematically reexamine these policies within the framework of institutional discussion of values of privacy and access. Undertaking such a process is discussed in greater detail later (see pages 34-37).

How the institution defines the boundaries of legitimate educational interest will depend on many factors, but it will be increasingly important to articulate such policy very carefully. As institutions continue to move toward the goal of having more information available for planning and decision-making, how can personally identifiable student information be protected against access that does not meet the institution's need-to-know definition?

[4] The Department of Education has created a model notification of rights under FERPA for postsecondary institutions (in FERPA Final Rule, *Federal Register*, November 21, 1996) that includes the following statement: "A school official has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibility." For more detail, see definitions for "Legitimate Educational Interest" and "School Official" in Appendix B, pages 40-41.

MISAPPLICATIONS OF PRIVACY

There are often misconceptions about privacy and its protection. Administrators should realize that privacy traditionally extends not to *all* information about an individual; rather the context determines what is considered private under the law. Privacy protection generally does not extend to persons who have died.

Privacy is a shield, not a sword. It ought not be a means for covering up wrongdoing or perpetuating a fraud. Often, among employers, there is a "conspiracy of silence," in which a representative of the institution is either untruthful, misleading, or noncommittal when asked about the work performance of a recently departed employee, including a student employed by the institution. This simply passes on an undesirable employee to another unknowing employer.

Such silence, which is sometimes blamed on "privacy," may actually stem from a fear of a later lawsuit based on defamation. But employers should realize that they would not lose such a lawsuit if they can defend the truth of what they have said or if it is clearly an opinion. An observation that "I would not hire the person again" or that "We would not recommend the person," whether written or verbal, raises little if any risk of later retaliation.

There have been cases in higher education of present or former students using the protection of the Family EducationalRights and Privacy Act to perpetrate a fraud. For instance, by asking a college or university not to release "directory information" about him, a student may lie to a prospective employer and say that he has a degree from the institution when he does not. The student expects that the federal law will render the institution powerless to set the record straight.

When asked whether the employment applicant received a degree, the campus official has some options, under the law:

(1) Answer by saying, "We have no information that we are permitted to disclose per student request."

(2) Suggest that the inquirer get the consent of the employment applicant to release his/her information.

So long as the official is not disclosing information from student records, s/he is on the safe side of the law.

Similarly, FERPA may make it difficult or impossible for different institutions to exchange information once they have been alerted to the possibilities of fraud perpetrated by a student or former student (for instance, a student who was admitted to a graduate school on the East Coast based on a fraudulent undergraduate record discovered at a West Coast institution). Many people believe that the only solution is an amendment to the federal law, permitting certain disclosures in order to correct erroneous assertions or to prevent the continuation of a fraud or deceit.

One public university registrar notes, "As institutions move toward networked information systems, the role of the student data steward becomes very complex and time-consuming. Perhaps the time is at hand to recognize the full-time profession of a student records data steward responsible for working with technicians in the development of systems which comply with policy, legal, and ethical standards; handling authorizations for system access, requests for student information, legal summons and subpoenas, and requests to withhold or release information for individual students; investigating complaints about inappropriate access or release of information or breaches of the security of the system itself; disposing of cases of outright fraud; and providing training in the legal and ethical handling of student data. To expect that all of these bases will be appropriately and consistently covered by individuals with other student service or technical responsibilities may be wishful thinking." Again, such choices about information practices will necessarily include a cost/benefit analysis.

Technology and Control

Implementations of technology — for example, a network-based information system — must incorporate the meaningful involvement of the relevant data stewards to guarantee their ability to control information

dissemination in accordance with the institution's defined need-to-know criteria. For example, personally identifiable student information may be accessible to someone classified as a "school official" without the student's prior consent. However, the definition of a school official may be vague, ambiguous, or not universally understood. It may permit inclusion of individuals such as affiliated legal counsel and contracted consultants. For these individuals, technology permits necessary and easy access to information while reducing institutional control of the dissemination of the information. While persons granted official access to protected information have an obligation equal to the data steward's to maintain privacy and confidentiality, they may not understand their responsibilities fully nor the implications of emerging technologies.

In addition to finding that technology may contribute to the complexity of exercising their stewardship responsibilities, data stewards may also find that some commercial information systems have limited mechanisms for providing access restrictions. Some institutions integrate student information in other information databases or displays. This commingling or merging of information presents challenges with regard to the principle of need to know in that certain personal information will require a higher level of access privilege. For example, a faculty advisor may have a legitimate need to access a student's grade information, but if the student's information is displayed with other information about the student to which the faculty member is not entitled access, this could violate the student's privacy.

In discharge of its stewardship responsibilities, and in design of its information systems, an institution needs to ensure that individuals be given access only to records they need, not to all information concerning a student or to the same information about all students, as in the incident below. This extends to routine, job-related access, as well as to special requests or circumstances necessitating access to student information.

A financial aid officer in a large midwestern university was pleased with the plan to reformat financial aid information and make it available to authorized individuals in the student's department. She believed this would make it easier for department personnel to discuss financial aid information with students directly and more conveniently. However, she found that the new application allowed all authorized personnel in all departments to access the financial aid information of all students. Insufficient input from this student services officer into the application development process resulted in greatly expanded potential access by many different individuals to student data and increased potential for privacy violations.

Examples of the Principle of Need to Know

Lesser Application ⟷ **Greater Application**

- ☆ The institution allows access to student information based on the legal constraints of FERPA.
- ☆ Student information is available through technology applications that have been minimally analyzed for compliance with the institution's privacy policies and procedures.

- ★ The institution has developed and published a data access policy that addresses legitimate educational interest and access responsibilities in a networked environment.
- ★ While appropriate staff members in each office have access to student information, the information is not readily transferred across different offices.
- ★ A custodial panel reviews and decides questions about legitimate educational purpose.

The incident also illustrates the importance of involving data stewards in the design and implementation of student applications to protect privacy.

4. Task Force Recommendations for Need to Know

◆ A clearly defined institutional policy should be adopted regarding access to student information, taking into consideration such criteria as job duties, purpose and scope of proposed use, and compliance with privacy regulations.

◆ Implementations of new technology applications should consider whether the system design supports institutional privacy policies and procedures, especially the design of display and report formats to limit the amount of information displayed on a screen.

◆ Technology implementations should include the active involvement of not only information technologists but also data stewards to ensure system design that supports need-to-know policy decisions.

The Principle of Data Accuracy, Inspection, and Review

1. Definition

The premise of the principle of data accuracy, inspection, and review is that information about students collected and maintained by a college or university must be accurate, and that students have the right to examine information about themselves and to request changes they feel should be made to their education records.[5] Without a sound approach to inspection and review, the institution will be hampered in meeting its requirement to correct information that is incorrect because input from students about the accuracy of their data will be lacking. A person cannot knowingly and meaningfully consent to the release of information in a record if s/he doesn't know what information is in the record.

2. Relevant Law

FERPA requires each institution (1) to permit a student "the right to inspect and review" education records; (2) to have an opportunity to challenge the accuracy of their records; and (3) as necessary, to include with the record a statement of dispute. Certain information is not subject to review. For example, substantive decisions such as grades or evaluations in lieu of grades are generally not subject to FERPA's amendment process. Laws in about twenty states permit a person to inspect his or her medical records. Further, institutions have an obligation to inform students each year of their rights under FERPA, which includes the right to inspect and review education records.

3. Policy Issues

The institution's responsibility with respect to this fair information principle is to define an effective request process and to make known to students the types of data that are being collected and maintained and the various offices responsible for the records to facilitate their request for review of their data. Within the context of FERPA, when a student asks to see his or her records, the institution must make the information available, unless there is a compelling and legally justifiable reason for non-release, and explain the information to the student during the inspection/review process. Methods for properly authenticating the identity of the student making the request should be in place prior to information release.

Two issues associated with this principle in a networked environment relate to responsibility for ensuring accuracy of student data in distributed databases, and the extent to which the right of inspection and review applies to data captured through transactions and automatic logging, including the feasibility and cost implications of such review.

Data Accuracy in a Distributed Environment

Technology has enabled student information to be replicated in a number of different databases, under the control of a number of different organizations within the institution. Since students have a vested interest in the accuracy of their own information, as well as the

[5] FERPA defines education records as those records, files, documents, and other materials which (1) contain information directly related to a student, and (2) are maintained by an educational agency or institution or a person acting for such agency or institution. (See the expanded definition of "Education Records" in Appendix B, page 40, for a list of records which are not considered education records under FERPA.)

right to inspect and review information stored about them, there is a certain logic in vesting primary responsibility for error detection with the student. However, the issue is more complex in a distributed environment. For while a student may be able to communicate to the steward of his or her information that a data element (for example, local address) is incorrect, it is unreasonable to expect the student to be cognizant of every office that may have replicated that information and to contact each one. The issue of how to synchronize or maintain currency of disparate databases is an institutional responsibility that must be addressed. Network technologies and network-based student systems can actually facilitate a student's access to his or her own data, and thus make it much easier for a student to inspect and review that data to be sure of its accuracy.

Review of Transactional Data

There are items of information now being collected about students that are not a part of the structured databases under the jurisdiction of student services and academic discipline officers — primarily data captured as a function of electronic transactions generated by student activity such as accessing a dining room or signing on to computer systems. To what extent is it possible to make such data available for student inspection and review? May a student request a modification to an event log, and how should such a request be handled? There may be costs associated with complying with student requests to inspect and review such records that the institution will need to address. Policies and procedures will be needed concerning these types of records, to define the records that can be made available and the related request and change process.

4. Task Force Recommendations for Data Accuracy, Inspection, and Review

◆ Students are responsible for providing accurate information about themselves for entry into college or university databases. However, institutions need to consider how distributed databases can be synchronized with the master data source so that students do not bear the responsibility for accuracy of their data in multiple databases. Institutions should also consider how such databases will be administered to increase consistency and employ good data management practices.

Examples of the Principle of Data Accuracy, Inspection, and Review

Lesser Application ⟷ **Greater Application**

- ☆ The institution responds once data inaccuracy is reported but places responsibility on the student for the accuracy of his or her data. Information is provided once by the source (student) and upon entry it is assumed to be valid unless the student specifies otherwise.
- ☆ There is no policy or set of guidelines in place to address data administration issues to ensure good data management practices.
- ☆ The institution does not systematically inform students of their right to inspect transational data for accuracy or have a process by which they can do this.
- ☆ The institution does not address the problem of data synchronization in a distributed environment.

- ★ The institution acknowledges its shared responsibility for data accuracy and spells out in policies or guidelines individual and institutional rights and responsibilities.
- ★ Data administration policy and procedures have been created to address the issue of data accuracy in a distributed computing environment.
- ★ The institution reveals all information being collected and facilitates student review of records, providing a convenient way to request a review. This is the case for all information, regardless of its sensitivity or how it is being collected.
- ★ The institution employs routine validity checks, and periodically asks students to review critical data.

◆ Institutions should periodically ask students to review critical data for accuracy, and should consider the use of secure technology to allow students direct access to their own data to facilitate inspection and review.

◆ Institutional policy and procedures should address the issues of inspection and review of transactional data, defining records that can be made available and the related request process.

Principle of Information Security, Integrity, and Accountability

1. Definition

The principle of information security, integrity, and accountability is composed of three related elements. *Security*, in terms of information technology, is the protection of user files and system resources from loss, damage, inappropriate access, and unauthorized disclosure or use of sensitive or private information. *Integrity* is reasonable assurance that data, once entered, will not be subject to unauthorized modification by intentional or unintentional means, and that data will remain unaltered during transmission between sending and receiving systems. *Accountability* in this context is the ability to explain security-related events and to link them to the originator. The cost of security, integrity, and accountability measures should be commensurate with the overall value of the information resource, and assessment of the overall risk posed by the existing or planned system or network implementation to the institution, to other sites, and to individual users' information.

2. Relevant Law

FERPA requires each institution not to disclose student information without written consent, except for certain specific uses and except for directory information, which may be disclosed unless the student objects. FERPA also requires each institution to maintain an audit trail within each student record listing all outsiders who have had access to the record and to keep that audit trail confidential, unless the disclosure is with consent or is limited to directory information. State computer crime laws provide punishment for the use of a computer in a crime and for unauthorized access to a computer system. The federal computer crime laws provide punishment for trafficking in stolen passwords and unauthorized access to a system across state lines. Fair information practice laws in several states require security of personal information in state institutions and, in some cases, the designation of a data security officer in each institution.

3. Policy Issues

Policy issues related to this principle arise in several areas, including appropriate levels of security for information of varying sensitivity; institutional policy for information access and acceptable use of electronic resources; and limitations and capabilities of the technologies employed.

Data and System Classification

Before institutions can begin to define adequate and reasonable security for their environments, there must be a shared understanding of which information is, in fact, sensitive and the degree of sensitivity. While legal and policy definitions may exist in the case of records in central student information systems or for research grants that contain explicit security provisions, the expansion of access to information generated by student activity or data in system logs introduces issues that may not yet have been considered. For example, how sensitive is student electronic mail? Is its protection to be a high priority or is it to be assumed and made known to students that unencrypted electronic mail is not private? How sensitive is a file about a student that is kept online by a faculty advisor? What security measures are appropriate for information the institution might require in an online application form (for example, family and background information, credit card number)? Is an individual's picture more sensitive when stored or disseminated electronically?

The rapid expansion in the number and character of items that may be shared electronically should evoke policy discussion on appropriate levels of security and sensitivity classifications for student information outside structured databases. The commonly used guideline has been: "If the information is personally identifiable, it must be protected." However, how the data will be protected and the measures that are reasonable for the assessed risks are institutional decisions that must be considered in light of the network environment and institutional culture. Moreover, assessment should be

made as to which systems are truly critical in the distributed environment (for example, ones whose loss or compromise would unduly jeopardize the security or integrity of private information or of other systems where private information is maintained).

As colleges and universities begin to transmit more and more information of a private nature to and about their students, the need to extend to academic networks the types of security that used to be associated primarily with administrative mainframe systems must be evaluated to avoid incidents such as the following.

The online student system at one eastern university was accessed for over two years by someone who knew how to work around newly implemented procedures. Sixty-eight grades for seven students were changed. Once the unauthorized access was detected, two employees were fired and three degrees were rescinded.

Responsible Use Policies

An institution must consider whether and how to define what it considers acceptable use of its information resources and how potential breaches in security or information privacy will be handled. Without a formal policy to define security rules, roles, and responsibilities, it may prove difficult to hold users accountable. Rules that are unwritten may also prove unenforceable.

Technical Capabilities and Limitations

In a nutshell, the primary security issue surrounding electronic transmission of private student information is: can information be ensured of privacy protection if the network itself is not at least reasonably secure? Having determined and defined appropriate uses (and abuses) of information and categories of sensitivity for both database records and data captured from tracking systems, how can the data be protected? Are there areas where limitations in existing security technology make a particular implementation unwise? Who will decide? In instances where technical security measures may be unavailable or inadequate, how will the institution gather user input on whether the value of access is more important than the risk of a privacy violation? How can individual choice to receive or not receive personal information electronically be accommodated?

Fundamental technical issues for heterogeneous networks of the type found in most institutions include authentication and authorization, communications security, physical security, and logging.

*Authentication and Authorizatio*n. What technical means can and should be employed to reliably validate the identity of network users (authentication) and to determine their access (authorization) levels? How can network access be controlled such that unauthenticated (and thus untraceable) access is eliminated, or services that can be obtained anonymously are limited to only those that can do little harm? How can individuals ensure that the electronic correspondence they receive is actually from the purported sender? How can an application determine it is connecting to the correct server and not to a system that has assumed its network identity? There are emerging cryptographic solutions in these areas (see page 11), but who will be responsible for planning their widespread introduction and use, and in what timeframe?

Communications Security. How can institutions safeguard private information being transmitted to or through traditionally less-controlled academic networks where students work? In particular, how can this be done in an era in which it is very easy for even amateur system crackers to "sniff" or read data from many unencrypted communications links? How can the institution ensure that applications developed in the distributed environment take into account communications security? How and where can technologies such as encryption be employed effectively, and how will institutional standards in this area be determined? Who is responsible for defining solutions to protect the privacy and integrity of student information on an institution-wide basis? What types of data integrity and checksumming measures are appropriate for information at the various sensitivity levels? Without a carefully planned strategy that facilitates protection of information as it is transmitted through the network, privacy may not be possible in any meaningful sense.

Physical Security. How will physical access to key network components, whose compromise could justify the privacy of attached networks, be controlled? If physical access can be gained to a major component of the network, or even to a PC where critical information is

Examples of the Principle of Information Security, Integrity, and Accountability

Lesser Application → **Greater Application**

- ☆ The network security function is not coordinated institution-wide, nor are information security concerns integrated into planning processes; security is left largely to individual system administrators.
- ☆ Automated error checking, audit trails, and purge criteria are not widely implemented.
- ☆ Formal risk assessment methodologies, vulnerability testing, security training, disaster recovery, and incident response strategies and responsibilities are not defined, or are ad hoc in nature.
- ★ The institution plans for and implements policy and processes to address the more critical physical and procedural security issues surrounding the dissemination of student information via networks.
- ★ Responsibilities for security are formally defined; security and integrity issues are integral and mandatory parts of the application design process at all levels.
- ★ Formal risk assessment methodologies, vulnerability testing, disaster recovery, incident response strategies, and responsibilities are defined.
- ★ The institution employs a confirmation process (such as digital signatures or encryption) that ensures student record information cannot be changed without detection while traveling across campus networks.
- ★ Automated error checking, checksums, audit trails, and purge criteria in some combination are routinely used.
- ★ Technical guidelines and training "how to's" related to security issues are provided to individual system administrators and to users.
- ★ Information management practices ensure that only authorized and authenticated staff members perform updates, and information is released only to authorized and authenticated requesters.

downloaded and stored — and there are no compensating security software products in place — private information can be read, modified, removed, or retransmitted. Policies should address the susceptibility to theft of components where sensitive data are kept.

Logging. A final technical network security issue is how much information about network transactions will actually be maintained. Because network intrusion detection is in its infancy, security events are seldom reported in real time. Thus, there is an increasing need for logs sufficient to reconstruct events weeks or even months after the fact. However, many of the systems that students commonly use may not yet employ an adequate level of logging to permit detailed reconstruction. Moreover, the logs themselves, if not properly managed, used, and secured may become a target or a potential privacy concern. How will accesses be logged and how much is appropriate and necessary to log (in keeping with the principle of minimization)?

4. Task Force Recommendations for Information Security, Integrity, and Accountability

◆ The institution should address the development of policies, processes, and procedures that deal with the more critical physical and procedural security issues surrounding the widespread dissemination of student information via networks.

◆ The institution should take reasonable steps to protect the integrity of student records by ensuring that they are not unduly subject to inadvertent or intentional modification or deletion when collected, stored, manipulated, displayed, or disseminated using the institution's electronic information resources.

◆ Responsibilities for security should be formally defined; security and integrity issues should be considered an integral and mandatory part of the application design process at all levels; and individual system administrators and users should be provided technical guidelines and training related to security issues.

◆ Care should be taken in setting up systems to avoid inappropriate — but in many cases built-in — information access, such as world-readable log files or Web caches not cleared from user to user.

◆ Institutions should articulate procedures for how potential breaches in security or privacy will be handled.

The Principle of Education

1. Definition

The premise of this principle is that colleges and universities have a basic responsibility to educate not only their students but faculty, staff, and administrators about the privacy rights of students and potential implications of use and misuse of personal information, especially in a networked environment. Students may not be familiar with these issues upon enrollment, and such understanding is necessary before they can give their informed consent for information use. This definition of "education" extends beyond simple notification and informed consent and includes information on the aspects of technology that may cause privacy concerns.

2. Relevant Law

FERPA requires each institution to inform students of their rights of privacy and access under the law. Each institution is also required to give public notice of the categories it has designated as directory information and therefore releasable unless the student objects.

3. Policy Issues

Administrators who handle arbitration of computer abuse incidents on college campuses have long recognized that more harm is done through ignorance about information technology than through a motivation to harm. Education, then, becomes a practical matter for the institution, if not an ethical matter. Such education regarding the privacy of student information in a networked environment means systematic instruction by the college or university to enable students to understand fully their privacy rights and the potential implications of uses and misuses of information.

There is a vast continuum between the legal requirement to inform students of what constitutes directory information and systematic instruction in privacy issues and technological impacts. If there were no legal obligations, what would the institution do? Colleges and universities will need to adopt an education policy somewhere along this continuum, based upon their culture, values, and commitment to an ethical approach.

Assessment of Educational Needs

Central to developing an educational program is assessing the current state of awareness by the student body and administration regarding privacy issues. Is there widespread awareness of the possible ramifications of providing increased electronic access to personal student information and an understanding that implicit tradeoffs exist between convenience and privacy? Is there an awareness that unencrypted electronic mail is not secure, or that e-mail may not be a privacy-protected entity on a given campus or in a given state? Are students knowledgeable enough about the World Wide Web to understand how the data and images posted there might be disseminated and subsequently used?

To what degree does the college or university wish to be responsible for helping its students become informed consumers of information technology, fully cognizant of both risks and benefits? How proactive does the institution want to be and what format will it use to

educate students with regard to privacy issues, including existing discipline and enforcement procedures, in the use of electronic information resources? Institutions will need to answer these questions as they formulate privacy education programs, especially to think about whether the tone of their program will be "educate to inform" versus "educate to warn."

Timing

When and how to reach students is an important issue in the formulation of an educational program, and the answers are probably unique to each campus. Many institutions provide information about computing during freshmen orientation, along with a deluge of other information ranging from parking to health services. This may be too much information to expect any individual to assimilate at one time. However, students usually want access to the Web and electronic mail services immediately upon arriving on campus, so it may be unwise to delay instruction about these services. How much information do students need immediately, and what information can be disseminated after freshmen orientation?

Dissemination Vehicles

Students may sign a statement during freshmen orientation that they agree to abide by the campus policy for ethical use of electronic resources. Receipt of a computing account may be contingent on this signing. If information isn't provided during freshmen orientation, what student communication vehicles (student government, student newspaper, campus radio station, institutional Web pages) are the most effective dissemination tools? What are the best mechanisms for reaching students within a particular institutional context? By what means do students receive information about the general policies of the institution and their responsibilities in networked environments, and how effective are these vehicles? For example, if an institution offers students an opportunity to opt out of getting their photo digitized, this option would best be explained to them on or near the time of the photo session. This form of education is in contrast to a sign posted in the back of the room which makes no mention of their choices, options, and access concerning such digitized photos.

Educating Faculty and Staff

Beyond education of the students, there remains an institution-wide process of raising the community's sensitivity to privacy, and to their individual responsibilities referred to by FERPA. When privacy education is mentioned, most people typically think about instructing students in these matters. But there is another population on campus that will likely need education on privacy issues as well — information handlers (including faculty) and technologists. Some unit or individual on campus should take responsibility for periodically providing professional development opportunities for data

Examples of the Principle of Education

Lesser Application ⟷ **Greater Application**

- ☆ The institution provides required notification about students' right to privacy in compliance with FERPA, probably through the student handbook or campus newspaper, but does not educate students further.
- ☆ The institution does not systematically attempt to educate faculty, staff, or administrators in legal or ethical privacy considerations.
- ★ The institution has developed an institutional process and delivers both a formal and informal instructional program that educates the entire community (not just students) about policies on privacy and the potential uses and abuses of technology in this regard.
- ★ The institution assumes the responsibility for assessing the effectiveness of this process/program.

handlers and technologists. While many professional organizations provide training/seminars/conferences on privacy issues, the campus has a role to play here, also.

4. Task Force Recommendations for Education

◆ Institutions should address the most effective methods in their environments to provide systematic instruction to students regarding their privacy rights and the potential implications of uses and misuses of information. Instruction should include information about aspects of the technology that may result in these uses and misuses, beyond simple notification and informed consent.

◆ The institution should ensure that faculty, staff, and administrators are also educated about the legal, ethical, and policy issues of students' right to privacy.

V. Building Policy in a Networked Information Environment

Our task force recommends that each college and university engage in a process to clarify the values that generally reflect its unique culture, mission, and environment (small or large, public or private, urban or rural), and to develop policy congruent with those values that addresses privacy issues in a networked information environment. How might a campus undertake such a process? Three key success factors are that the process be open, that it have executive-level support, and that the discussions be based on real incidents.

An Open Process

It is important that the process of building policy about handling information in a networked environment be institution-wide and open, that is, involve many different campus constituents — faculty, staff, students, administrators. Both technologists and non-technologists should participate in these discussions to fully explore the implications of a networked information environment, identify relevant laws, clarify values, and weigh potential tradeoffs.

Several colleges and universities have developed model policy-building processes (primarily for developing policies addressing broader networked information resources issues, including privacy). Four campus experiences are described below.

.

Cornell University

Cornell University relies on fundamental principles and mission when developing any policy. Both computer use and abuse policies have been created to conform to the University's existing understanding of issues and to reflect Cornell's culture. The best way to ensure this outcome is to include community members in its creation. At Cornell this process is multi-stepped.

The process used to develop Cornell's electronic resources policy began with the Vice President of Information Technologies asking the Associate Vice President for Human Resources, the University Counsel's Office, the Judicial Administrator, and several representatives from the Information Technologies organization to join him in discussion about responsible use of electronic communications. These discussions, which occurred over the course of a year, took into consideration existing relevant University policies, codes, guidelines, and practices, and resulted in the drafting of a policy. This draft policy was then reviewed by faculty members, staff, and students prior to its implementation. The Dean's Council, the Faculty Committee of Representatives, and the University Assemblies (representing the students, faculty, and staff) all discussed and had input into the revisions of the draft policy. After such wide campus involvement, the ratification process was smooth, paving the way for implementation and education.

Implementation and education are as important as

the policy creation, especially since there is a computer use culture that often runs counter to institutional policies and state and federal laws. At Cornell, all new students attend a 50-minute education program to learn about and discuss electronic communications and computer resources on campus. Part of this course focuses on responsible use issues. In addition, the office of Information Technologies provides educational programs to the colleges, including the deans, directors, and department heads as well as system administrators and student groups. The programs provided at Cornell that were the most well attended in 1996 focused on the Communications Decency Act and included discussions on censorship, freedom of expression, privacy, and ethical use of computer resources. For more information, contact Marjorie Hodges at mwh2@cornell.edu or see http://WWW.UNIVCO.CORNELL.EDU/policy/RU.html

University of Maryland at College Park

The University of Maryland at College Park is the flagship campus of the University of Maryland System. The campus administration does not adhere to a single policy-making process but offers a variety of avenues by which policy can be developed. Decision-making is notably decentralized at an institution that includes thirteen colleges and schools and three administrative deans who manage programs in a cooperative administrative structure.

The College Park Senate provides an opportunity for faculty, staff, students, and administrators to participate in campus governance. While, to date, the Senate's role in the development of technology policy has been minimal, it has the potential for providing the forum necessary for open and inclusive deliberations. A data policy committee has also been established to develop guidelines and policies governing the development and management of campuswide data and databases. Some policies are developed from grass-roots efforts; the *Guidelines on the Acceptable Use of Computing Resources* resulted from the work of a group of faculty, administrators, and staff and the review of legal counsel, cabinet, and Dean's Council.

Project NEThics, a new initiative of Academic Information Technology Services, provides a model for open community discussion and examination of issues. The Project's mission is to ensure responsible use of University computing resources through policy enforcement and user education designed to inform community members about the legal and ethical implications of computer use. Project NEThics staff play a key role in pulling together policy-makers and users from across the campus to stimulate dialogue in this area. Given the University's ambiguous policy structure and a persistent campus culture that favors decentralized decision-making and authority, it is expected that Project NEThics' efforts to coordinate policy development will be vital to the establishment of technology policy that maximizes input, ensures the support of upper-level administration, and is based upon real incidents. For more information about this model, contact Rodney Petersen at rodney_j_petersen@umail.umd.edu or see http://www.inform.umd.edu:8080/CompRes/PolicyAndEthics/aug/

University of Michigan

The University of Michigan is also a highly decentralized environment. There are three campuses within the University system. The largest campus, in Ann Arbor, has seventeen schools and colleges, each with its own administrative decision-making processes. The University has a large, diverse community of approximately 80,000 faculty, staff, and students.

Information technology policy has been made through a combination of efforts, mostly committee centered. Committees, representing faculty, staff, and students, have been assembled to gather information, discuss, and formulate recommended policy on such issues as responsible use of technology, privacy of electronic mail, definition and handling of electronic records, handling of personal information, and data administration. All policy recommendations are also reviewed by legal counsel, and most also by the campus Civil Liberties Board, Faculty Senate, Council of Deans, and other relevant groups. Even with such committee involvement, however, achieving adequate input and response from the campus community is a significant challenge.

A model which has been successfully used at the University of Michigan, called the "Think About It Campaign," has provided a mechanism for expanding the debate of important issues and increasing both input to the formulation of policy and commitment to the established policies. In this model, faculty, staff, and student volunteers are recruited to facilitate, in pairs, small and large group discussions of ethical issues related to tech-

nology use on campus. The volunteers are trained in group facilitation techniques and given an opportunity to debate the issues themselves prior to being assigned a group. Real vignettes, illustrating technology-related ethical dilemmas such as conflicts between ease of use and security, between freedom of speech and freedom from harassment, and between censorship of content and unlimited access, are provided as discussion starters. The key component of this model is that discussion is the goal in and of itself, not necessarily finding the "right" answer. In this way, participants are made comfortable sharing their points of view and the community view is allowed to emerge. For more information about this model, contact Virginia Rezmierski at ver@umich.edu or see http://www.cause.org/information-resources/ir-library/text/cem9233.txt

University of North Carolina-Chapel Hill

The University of North Carolina-Chapel Hill, another large and complex community, has successfully used an open process to develop a policy framework for networked information. The Information Resources Coordinating Council (IRCC) at the University of North Carolina was created by the chief financial officer to coordinate the management of pan-University digital information stores and technologies distributed across organizational boundaries. The committee reviewed issues and principles which had previously been developed by a faculty-based advisory committee. They developed a policy framework to guide ongoing development of information policy. The council of library and technology leaders then initiated a series of discussions with representative focus groups, administrative units, and governance councils. Participants in these discussions received advance copies of the draft policy along with descriptions of several information-related campus incidents. These incidents/cases served to highlight implications and tradeoffs inherent in the policy framework and to underscore the need for such a document. Finally, after these extensive open campus discussions, the Chancellor's Administrative Council endorsed the policy framework for the campus.

Implementation of this policy framework is also being done through an open, participatory process. The IRCC has commissioned several working groups to begin the implementation process. One group is focused on the scope, integrity, and presentation of "official" institutional data, another on coordinating departmental and special interest Web pages, another with recommending institutional standards for imaging applications, and another on privacy. For more information about this model contact Anne Parker at anne_parker@unc.edu or see http://www.cause.org/information-resources/ir-library/text/cem9524.txt

Other resources

Researching the way other institutions have dealt with developing policy about privacy and other issues that arise in an electronic networked environment can be a valuable part of the process of policy building in this area. In addition to the experiences described here, several other resources on the World Wide Web are worth investigating. The University of Pennsylvania offers an excellent set of privacy resources, including the report of Penn's privacy task force, on their Web site (see http://www.upenn.edu/security-privacy/privacy.html). In addition, as part of the work of our CAUSE task force, a Web site at the University of Texas/Austin was developed to provide an index and hypertext links to nearly 100 policies that deal with privacy of student information at various colleges and universities, indexed by state location (see http://www.utexas.edu/computer/vcl/projects/privacy.html).

Also, at the CAUSE Web site (http://www.cause.org/) is a resource page that provides links to networked information policies that have been contributed to the CAUSE Information Resources Library, many of which are available electronically on the Web and linked from that page. The page (at http://www.cause.org/issues/policy.html) provides other related resources, such as links to the Electronic Frontier Foundation's guidelines for computing policies and sites addressing first amendment issues. Appendix H provides additional resources.

Highest Level Support

In addition to being an open process, the task force recommends that it be supported publicly at the highest levels of the college or university administration. Executive officers may even want to go beyond public endorsement of the process, actively receiving output from the discussions and/or personally charging groups to research and debate selected topics such as technology-related risk management and cost analyses, effects of

process reengineering on privacy, and others.

Risk management discussions are important with respect to the security, integrity, and accountability of data. The acceptable risk level for one campus may be too great for another. Open discussions in this area can help to identify risks and clarify community values regarding acceptable and unacceptable risk levels. They can also help to identify ways in which technology might be deployed to reduce or eliminate risks for both individuals and the institution. It will be important to explore the costs of implementing security technologies compared to the potential costs of liability resulting from a violation of privacy. Open discussion of these and other values-related topics can help colleges and universities in strategic planning to identify those areas in which the greatest investment will reap the greatest benefits in line with institutional values and mission.

Seeing more efficient and effective ways of doing business has led some institutions to engage in process reengineering, which usually involves technology applications. Open discussion of the challenges facing colleges and universities that lead to process reengineering can foster increased understanding, community trust, and endorsement of the new processes. The partnerships that are established between data stewards, data owners, data users, and technology designers can be invaluable when they result in new and creative ways to maximally meet both the needs of the student/customer and the institution.

College and university communities will also be able to steer the identification and initiation of needed technological pilots if there are open discussions about these issues. Identifying units within colleges that are ready and eager to pilot new applications and discuss the pilot results can facilitate the process of evaluating new applications. Encryption and digital signature technology pilots are among those that may help campuses apply technology to protect privacy. Finding out whether such technologies will prove cumbersome to the community or be embraced by it would be enormous benefit before wide scale applications are implemented.

Based on Real Incidents

Finally, our task force recommends that values clarification and development of policy be based on specific incidents and issues. Sometimes a campus does not want to make public the incidents of misuse or abuse that have occurred for fear of liability for errors in information delivery or access that find one person in the middle of another's sensitive data. However, the community needs to be able to understand and relate directly to the issues at hand. More information shared, rather than less, will help to build community consensus and standards. At a minimum, information needs to be disseminated to the community to spark discussion — information about the dilemmas and any potential tradeoffs faced by the institution between efficiency and individual privacy. If it is an open and listening process, one of forming consensus and sharing different points of view, the community as a whole benefits with increased commitment to community values and the development of informed and supported policies

Appendix A: FERPA Overview

The information below is excerpted from the *Guidelines for Postsecondary Institutions for Implementation of the Family Educational Rights and Privacy Act of 1974 as Amended,* edited by Richard Rainsberger, published by and available from the American Association of Collegiate Registrars and Admissions Officers (AACRAO, One Dupont Circle, NW, Suite 330, Washington, DC 20036-1171; 202-293-9161). Periodically amendments are made to FERPA regulations; the Department of Education's Web site provides access to such changes in the Federal Register Documents section under News (at http://www.ed.gov/news.html).

The purpose of the Family Educational Rights and Privacy Act of 1974, commonly referred to as the Buckley Amendment or FERPA, is to afford certain rights to students concerning their education records.

FERPA gives students who reach the age of 18 or who attend a postsecondary institution the right to inspect and review their own education records. Furthermore, students have other rights including the right to request amendment of records and to have some control over the disclosure of personally identifiable information from these records. Institutions may grant a student more rights than those guaranteed in the Act.

Institutions may not disclose information contained in education records without the student's written consent except under conditions specified in the Act. An institution is not required to disclose information from a student's education records to the parents of dependent students but may exercise its discretion to do so. It is the responsibility of an institution to ensure that information is not improperly disclosed to the parents of students.

Institutions must annually notify students currently in attendance of their rights by any means that are reasonable, such as publication of a notice in the student handbook, catalog, or student newspaper. The regulations do not specify the means to be used. Schools are not required by FERPA to notify former students of their FERPA rights.

FERPA deals specifically with the education records of students, affording them certain rights with respect to those records. For purposes of definition, education records are those records which are (1) directly related to a student and (2) maintained by an institution or a party acting for the institution. Records containing a student's name, Social Security number, or other personally identifiable information, in whatever medium, are covered by FERPA unless identified in one of the Act's excluded categories (see the definition of "Education Records" on page 40).

Educational institutions and agencies are required to conform to fair information practice. This means that persons who are fair subjects of data systems (i.e., students at an institution) must:

- be informed of the existence of such systems,
- have identified for them what data about them are on record,
- be given assurances that such data are used only for intended purposes,
- be given the opportunity to request an amendment or correction to their records, and
- be certain that those responsible for data systems take reasonable precautions to prevent misuse of the data.

Although the Act does not require it, those responsible for data systems are obliged to consider properly disposing of, or destroying, information when the conditions under which that information was collected no longer exist and there are no legal restrictions preventing such disposal.

FERPA applies to all schools that receive funding under most programs administered by the Secretary of Education. Most postsecondary institutions, both public and private, generally receive such funding and must, therefore, comply with FERPA.

Appendix B: Glossary of Terms

Authentication
A process that verifies the identification or genuineness of a person or service. Traditionally, authentication methods in networked computer systems include a user ID/password combination ("something you know"), a token ("something you have"), and/or biometrics identification ("something you are and cannot change").

Authorization
Access permissions or rights given to a user, process, or program. Usually, authorization is used in conjunction with the concept of authentication. Once a user has been authenticated, s/he may be authorized to have different types of access or activities.

Checksum
A computed value which depends on the contents of a block of data and which is transmitted or stored along with the data in order to detect corruption of the data. The receiving system recomputes the checksum based upon the received data and compares this value with the one sent with the data. If the two values are the same, the receiver has some confidence that the data were received correctly.

Data Mining
Analysis of data in a database using tools that look for trends or anomalies. These data can then be extracted in such a way that the new information is used for decision support, prediction, forecasting, and estimation.

Data Steward
Person or entity responsible for the management, integrity, and safeguarding of information. Data stewards have evolved to include not only traditional stewards such as registrars for student data, but also such people as database administrators.

Data Warehouse
A collection of data extracted from one or more production databases, housed in a separate database, providing fast and easy user access to "high-demand" information.

Digital Signature
Extra data appended to a message that identify and authenticate the sender and message data using public-key encryption.

Digitized Photograph
A photograph recorded in binary code and stored on computer-compatible media (for example, disk, tape, CD-ROM). Digitized photos are particularly easy to enhance, modify, or manipulate. Such photos can be stored in a database, outputted as a print or transparency, or converted for video-screen display from a CD-ROM or photo CD.

Digitized Signature
Image replicas of an individual's own handwritten signature obtained during a signing operation (much like the pads/signature recording devices beginning to be employed by major department stores).

Directory Information
Information about students of an institution that is considered part of the public record of their attendance and that may be made public unless the student specifically asks that it be suppressed. This may include some or all of the following: name, local address, local phone number, e-mail address, major field of study, participation in recognized activities and sports, weight and height of athletic team members, photograph, dates of attendance, most recent institution attended, degrees and awards received.

Disclosure
Permitting access to or the release, transfer, or other communication of personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic means.

EDI (Electronic Data Interchange)
A technology that uses standard data formats to transmit data from one computer to another. In higher education, EDI has been used to transmit student transcripts.

Education Records*
Those records directly related to a student and maintained by the institution or by a party acting for the institution. The term "education records" does not include the following:

- records of instructional, supervisory, administrative, and certain educational personnel which are in the sole possession of the maker thereof, and are not accessible or revealed to any other individual except a substitute who performs on a temporary basis (as defined in the institutional personnel policy) the duties of the individual who made the records.
- records maintained by a law enforcement unit of the educational agency or institution that were created by that law enforcement unit for the purpose of law enforcement.
- records relating to individuals who are employed by the institution, which are made and maintained in the normal course of business, relate exclusively to individuals in their capacity as employees, and are not available for use for any other purpose. (Records of individuals in attendance at an institution who are employed as a result of their status as students are education records, for example, workstudy.)
- records relating to a student which are (a) created or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional, acting in his/her professional capacity or assisting in a paraprofessional capacity; (b) used solely in connection with the provision of treatment to the student; and (c) not disclosed to anyone other than individuals providing such treatment, so long as the records can be personally reviewed by a physician or other appropriate professional of the student's choice. (Appropriateness may be determined by the institution.) "Treatment" in this context does not include remedial educational activities or activities which are part of the program of instruction at the institution.
- records of an institution that contain only information relating to a person after that person is no longer a student at the institution (for example, information gathered on the accomplishments of alumni).

Encryption
Any procedure used to convert plain text into cipher text in order to prevent any but the intended recipient from reading that data.

Identification
Any means of identifying an individual, physical or automated. A process that enables recognition of an entity by an automated information system is generally accomplished through the use of unique machine-readable user names.

Informed Consent
Permission given by an individual to another for some action, with such consent being well-founded in information and knowledge about the issues.

Legitimate Educational Interest
FERPA does not define "legitimate educational interest" but states that institutions must establish their own criteria according to their own procedures and requirements for determining when their school officials have a legitimate educational interest in a student's education records. However, the Department of Education has created a model notification of rights under FERPA for postsecondary institutions (in FERPA Final Rule, *Federal Register*, November 21, 1996) that includes the following statement: "A school official has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibility."

Log File
A collection of information, generally of machine and user activities, that shows sequence of machine transactions.

Middleware
Software that mediates between an application program and a network. Such software manages the interaction between disparate applications across heterogeneous computing platforms.

Monitoring
Watching or recording activity on a particular machine or network or by a particular user or set of users usually for system management purposes.

Personally Identifiable*
Data or information which include (1) the name of the student, the student's parent, or other family members; (2) the student's address; (3) a personal identifier such as a Social Security number or student number; or (4) a list of personal characteristics, or other information which would make the student's identity easily traceable.

Profiling
The process of gathering information about a particular individual or class of individuals for purposes of outlining/highlighting data such as their potential product interests or ability/desire to contribute to a particular philanthropy.

Record
Any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche.

School Official
FERPA does not define "school officials" but states that institutions must establish their own criteria according to their own procedures and requirements for determining them. However, the Department of Education has created a model notification of rights under FERPA for postsecondary institutions (in FERPA Final Rule, *Federal Register*, November 21, 1996) that includes the following description of a school official: "A person employed by the University in an administrative, supervisory, academic or research, or support staff position (including law enforcement unit personnel and health staff); a person or company with whom the University has contracted (such as an attorney, auditor, or collection agent); a person serving on the Board of Trustees; or a student serving on an official committee, such as a disciplinary or grievance committee, or assisting another school official in performing his or her tasks.

Sniffing
A process accomplished by a non-intrusive technical device, difficult to detect, placed on a network segment which collects and stores all data moving across that segment for later analysis and unauthorized use. Sniffing can be a legitimate and authorized tool for solving network problems, but it can also be misused.

Student*
Includes any individual for whom an educational institution maintains education records. The term does not include an individual who has not been in attendance at the institution. An individual who is or has been enrolled in one component unit of an institution, who applies for admission to a second unit, has no right to inspect the records accumulated by the second unit until enrolled therein.

World Wide Web (WWW)
A client/server software package which uses hypertext to organize, connect, and present information and services throughout the Internet.

---

* This definition is excerpted from AACRAO's *Guidelines for Postsecondary Institutions for Implementation of the Family Educational Rights and Privacy Act of 1974 as Amended.*

Appendix C: Summary of Task Force Recommendations for Each Principle of Fair Information Practice

Recommendations for Notification

◆ Institutions should notify students of their privacy rights with the same prominence and frequency afforded other important areas of campus life, such as residence-hall regulations, meal-plan options, and course descriptions. A useful comparison may be made between notification of campus judicial system regulations, which focus on student responsibilities and punishment, and notification of privacy policies about student records, which focus on student rights and abilities.

◆ The institutional approach to notification should also take into account the technological sophistication of the student body. This and other local considerations should be applied in order to provide useful and meaningful information to students. An effort should be made to avoid overwhelming detail on the one hand and overly vague generalities on the other.

◆ When formulating policies and procedures concerning student notification, campuses should consider the effects of the distribution of databases to non-centrally controlled systems, as well as transaction and tracking data maintained as a by-product of daily operations. Policy should determine how students can be informed of the existence of such databases and systems.

Recommendations for Minimization

◆ Colleges and universities should gather all legally required student information and the minimal amount of additional information to accomplish a legitimate institutional purpose, avoiding gathering nonessential information simply because of the ease of collection or correlation in networked environments. Policy and practice should address means to ensure that collection of personally identifiable information has been appropriately authorized.

◆ Campuses should formulate a process for determining necessary log elements and log retention requirements, particularly for logs where the inclusion of personally identifiable information is unavoidable.

◆ For those log elements over which the institution exercises control (rather than those that are a default of the operating system or vendor-supplied software), designers should consider the principle of minimization and identify those elements that would really be necessary in the event of foreseeable contingencies. Those elements rather than the superset of all possible elements should be collected.

Recommendations for Secondary Use

◆ The institution should be explicit about the purpose for which information is gathered at the time of its collection, and identify the routine and compatible uses of the data it expects to employ in the course of conducting official business.

◆ Secondary uses, not included in those stated as routine and compatible, should be avoided, but where such secondary uses are deemed significantly important to the institution, policy should consider how additional permissions will be obtained from affected students.

Recommendations for Nondisclosure and Consent

◆ During policy development, institutions should consider defining categories of information as to their sensitivity, determining under which strata elements of information fall, and establishing congruent consent/disclosure mechanisms for each type of information.

◆ In developing policy with regard to data categorization, institutions should consider the means for students to change the categorization of an element and to specify that it be treated as more sensitive than generic policy would normally dictate. The use of technology to facilitate individual choice in this area should be considered.

◆ Consent should be specific with regard to the manner and type of disclosure, as well as the identity of the recipients and their intended use of the information. The means by which students may revoke consent should be addressed during the policy development process.

◆ The institution should ensure that students fully understand what their rights are with regard to requesting that information not be disclosed.

Recommendations for Need to Know

◆ A clearly defined institutional policy should be adopted regarding access to student information, taking into consideration such criteria as job duties, purpose and scope of proposed use, and compliance with privacy regulations.

◆ Implementations of new technology applications should consider whether the system design supports institutional privacy policies and procedures, including the design of display and report formats to limit the amount of information displayed on a screen.

◆ Technology implementations should include the active involvement of not only information technologists but also data stewards to ensure system design that supports need-to-know policy decisions.

Recommendations for Data Accuracy, Inspection, and Review

◆ Students are responsible for providing accurate information about themselves for entry into college or university databases. However, institutions need to consider how distributed databases can be synchronized with the master data source so that students do not bear the responsibility for accuracy of their data in multiple databases. Institutions should also consider how such databases will be administered to increase consistency and employ good data management practices.

◆ Institutions should periodically ask students to review critical data for accuracy, and should consider the use of secure technology to allow students direct access to their own data to facilitate the inspection and review process.

◆ Institutional policy and procedures should address the issues of inspection and review of transactional data, defining records that can be made available and the related request process.

Recommendations for Information Security, Integrity, and Accountability

◆ The institution should address the development of policies, processes, and procedures that deal with the more critical physical and procedural security issues surrounding the widespread dissemination of student information via networks.

◆ The institution should take reasonable steps to protect the integrity of student records by ensuring that they are not unduly subject to inadvertent or intentional modification or deletion when collected, stored, manipulated, displayed, or disseminated using the institution's electronic information resources.

◆ Responsibilities for security should be formally defined; security and integrity issues should be considered an integral and mandatory part of the application design process at all levels; and individual system administrators and users should be provided technical guidelines and training related to security issues.

◆ Care should be taken in setting up systems to avoid inappropriate — but in many cases built-in — information access, such as world-readable log files or Web caches not cleared from user to user.

◆ Institutions should articulate procedures for how potential breaches in security or privacy will be handled.

Recommendations for Education

◆ Institutions should address the most effective methods in their environments to provide systematic instruction to students regarding their privacy rights and the potential implications of uses and misuses of information. Instruction should include information about aspects of the technology that may result in these uses and misuses, beyond simple notification and informed consent.

◆ The institution should ensure that faculty, staff, and administrators are also educated about the legal, ethical, and policy issues surrounding students' right to privacy.

Appendix D: Checklist for Privacy Policy and Fair Information Practices

The following is a checklist that will help guide the development or revision of policies on the handling of student information to ensure privacy and confidentiality. The task force suggests that the items below be addressed within the process outlined in section V, and within the framework of recommendations for policy and practice summarized in Appendix C.

The Principle of Notification

___ We have established procedures for notifying students about their privacy rights and responsibilities in a networked environment.

___ We have established procedures for notifying students about disciplinary action that will be taken when students violate the privacy rights of others.

___ We have established procedures for notifying students about what data are considered "directory information" and the medium for publishing such information — paper, campus intranet, public network.

The Principle of Minimization

___ We have a policy that addresses logging and/or monitoring individually identifiable online transactions and activity of students.

___ We have a policy that addresses logging and/or monitoring individually identifiable online transactions and activity of students at public workstations in computer labs.

___ We have established procedures for approving on-campus research using online data, including collecting data about how students use the campus network.

___ We have an institution-wide policy that addresses issues related to the sources, collection, storage, and purging of student information in a networked environment.

___ We have a policy about the collection of contingency data to manage institutional risk.

The Principle of Secondary Use

___ We have a policy about what students should be told at the time of enrollment about possible secondary use of information they provide.

___ We have a policy that addresses the potential to create new, potentially confidential information from existing data that have been collected by the institution.

___ We have defined the routine and compatible uses of data the institution expects to employ in the course of conducting official business.

The Principle of Nondisclosure and Consent

___ We have a policy that addresses nondisclosure and consent issues that arise in a networked environment, such as what information may be posted on the World Wide Web, with or without consent, and by whom.

___ We have a policy on nondisclosure and consent that addresses institutional ownership versus student ownership of such student information as digitized signatures and photographs.

___ We have a policy that addresses issues of sensitivity of data, congruent consent/disclosure mechanisms, and the ability of students to request that data be treated as more confidential or to revoke consent.

___ We have a policy that addresses requests for access to student records by parents.

___ For the purpose of consistency among our policies, we have defined what constitutes an "emergency request" for student e-mail or other electronic records.

___ We have a policy outlining procedures for handling subpoenas requesting access to student e-mail and computer records.

____ We have a policy that addresses the confidentiality of electronic mail and articulates standards for handling e-mail by system administrators and others in the campus community.

____ We have a policy that addresses what types of information are appropriate for transmission by electronic mail.

The Principle of Need to Know

___ We have an institution-wide policy about access to student information that includes definition of a school official and what the institution considers legitimate educational interest, to guide decisions about who has a "need to know."

___ We have procedures in place to ensure that new or reengineered automated systems will support privacy rights.

___ We have identified which administrators can approve a search of student e-mail boxes or confidential records.

___ We have identified who may have access to systems transactions and under what circumstances (for example, monitoring for the purposes of system administration).

___ We have a policy requiring frequent review of job categories for need-to-know access.

___ We have a policy requiring a review of need-to-know status when databases are created or merged.

___ We have a policy about which administrators can have access to student disciplinary information in computer abuse cases.

The Principle of Data Accuracy, Inspection, and Review

___ We have a policy and procedures about when and how students can change their own online directory information.

___ We have a policy and procedures that address the administration of multiple and/or distributed databases to ensure good institution-wide data management practices.

___ We have a policy and procedures that address the issues of inspection and review of transactional data.

The Principle of Information Security, Integrity, and Accountability

___ We have a policy on the security of passwords.

___ We have identified authentication methods for online commerce.

___ We have a policy regarding level of security/encryption required for sensitive data transmitted through the campus network.

___ We have a policy regarding level of security/encryption required for sensitive data transmitted through public/untrusted networks.

___ We have a policy with regard to integrity checks for sensitive or mission-critical data transmitted through the campus network or through public/untrusted networks.

___ We have policies regarding appropriate host and network security geared to the sensitivity of data.

___ We have identified and publicized appropriate sanctions to be levied in cases where students alter online data owned by the institution or data of other students.

___ We have a security policy that formally defines responsibilities for security, encourages the consideration of security in applications development and design, and articulates procedures for how potential security breaches will be handled.

___ We have a training program that ensures that system administrators and users are provided technical guidelines related to security issues.

The Principle of Education

___ We have established a program to provide instruction to students about their privacy rights and the potential implications of uses and misuses of electronic information resources, including awareness about the institution's policy on e-mail confidentiality.

___ We have established an educational program to ensure that faculty, staff, and administrators are educated about the legal, ethical, and policy issues surrounding students' right to privacy.

Appendix E: Additional Information Principles

A Code of Fair Information Practice

The following code of fair information practice is excerpted from House Report 103-601 Part V and is derived from several sources, including codes developed by the Department of Health, Education, and Welfare (1972 report); Organization for Economic Cooperation and Development (1981); and the Council of Europe Convention (1981). It was provided to our task force by privacy and information policy consultant Robert Gellman.

1. The Principle of *Openness*, which provides that the existence of record-keeping systems and data banks containing data about individuals be publicly known, along with a description of main purpose and uses of the data.

2. The Principle of *Individual Participation*, which provides that each individual should have a right to see any data about himself or herself and to correct or remove any data that is not timely, accurate, relevant, or complete.

3. The Principle of *Collection Limitation,* which provides that there should be limits to the collection of personal data, that data should be collected by lawful and fair means, and that data should be collected, where appropriate, with the knowledge or consent of the subject.

4. The Principle of *Data Quality*, which provides that personal data should be relevant to the purposes for which they are to be used, and should be accurate, complete, and timely.

5. The Principle of *Use Limitation*, which provides that there must be limits to the internal uses of personal data and that the data should be used only for the purposes specified at the time of collection.

6. The Principle of *Disclosure Limitation*, which provides that personal data should not be communicated externally without the consent of the data subject or other legal authority.

7. The Principle of *Security*, which provides that personal data should be protected by reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification, or disclosure.

8. The Principle of *Accountability*, which provides that record keepers should be accountable for complying with fair information practice.

Principles of Information Privacy

By Robert Ellis Smith, Publisher, *Privacy Journal*

Information collectors are constantly saying, "Privacy is a vague concept. It means different things to different people." In fact, over the past two decades a substantial amount of study has gone into privacy issues — always with an eye to developing principles that will guide those who develop information systems. Some of the principles that follow have widespread agreement among experts in the privacy field; others are fairly new and untested.

1. There must be no personal-information systems whose very existence is secret.

2. There must be a way for a person to find out what information about him or her is in a record and how it is used.

3. There must be a way for a person to prevent personal information that was obtained for one purpose from being used or made available for other purposes without the consent of the person.

4. There must be a way for a person to correct or amend a record of identifiable information about the person.

5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the information for its intended use and must take precautions to prevent misuse of the data.

6. Any systems of records about people must have a purpose that is socially desirable, and only relevant information should be collected.

7. To the maximum extent, personal information should be gathered from the individual himself or herself.

8. The keepers of personal information should act in the role of trustee, safeguarding the information and using it in the best interests of the individual but not "owning" it.

9. Privacy interests should be considered specifically in the design and creation of new data systems, communications services, and other new technology that affects the interests of individuals.

10. Privacy protections, as much as possible, should be tailored to the needs of each individual, and each individual should be able to choose from among various degrees of privacy protections, perhaps bearing an additional cost for special services.

11. A company or government agency that compromises current expectations of privacy should be obligated to offer a means of restoring the lost degree of privacy at no cost to consumers.

12. Information provided to a business or government agency by a person should be used only in connection with services or benefits sought by the person, unless the person agrees otherwise.

13. Privacy expectations may change over time, as new technology, new markets, new attitudes, and new social concerns emerge.

14. When information is disclosed for commercial purposes, an individual ought to have a means to "opt out" by having his or her information not disclosed.

15. The concept of privacy applies only to actual persons, not to organizations. It applies only to information that identifies an individual (by name, number, or otherwise), not to cumulative or anonymous information.

16. Privacy problems lend themselves to negotiation and complaint resolution, often on a case-by-case basis, rather than hard-and-fast legal language.

17. Personal information provided to a third party (for processing or billing or research) is governed by the same protections applicable to the original keeper of the records.

18. Personal information may be transferred from one country to another only if the second country has privacy protection at least equal to those of the first country, unless the first country provides special permission.

19. Information used by a government agency should be available to citizens in two formats: in the media (whether electronic or otherwise) used by the agency itself, and in the form that is usable and readable to a person without electronic media.

20. In the absence of factual suspicion, overhearing private conversations or viewing people's personal activities from afar with technological enhancements is unethical.

Sources:

The first five principles of information privacy were originated by a study committee in the U.S. Department of Health, Education, and Welfare in 1973, and endorsed later by an IBM Corporation study and by the organization of Computer Professionals for Social Responsibility. This "Code of Fair Information Practice" appears again and again in laws passed since 1973, including the federal Privacy Act, state fair information practice acts, and national laws enacted by European countries.

Principle 6 is part of the 1981 privacy guidelines of the Organization for Economic Cooperation and Development (OECD) in Europe.

Principle 7 is part of the federal Privacy Act.

There is less agreement about Principle 8, which is not yet a part of any recognized code of practice.

Principles 9-13 are based on principles published in 1991 by the New York State Public Service Commission, under the leadership of Commissioner Eli Noam. Principles 10 and 11 together mean that customers or citizens should not have to pay to preserve the privacy status quo; however, customers or citizens choosing a greater degree of protection should expect to bear at least part of the cost themselves. Many European nations have adopted a variation of Principle 12, saying that an individual is entitled to know from the beginning the purpose for information he is asked to provide.

Principle 14 is promoted by the direct-marketing industry and others. It begs the question of whether people know the consequences of "opting out" and whether information should be collected or disclosed at all.

The first part of Principle 15 is a general concept of law. Businesses may have an interest in secrecy or confidentiality but this is different from the uniquely individual right of privacy.

In the U.S. there is no general agreement on Principle 16, which seems to guide policy makers in Europe, Australia, and Canada.

Principle 17, part of the federal Privacy Act, assures that processing or research organizations merely act as the agent of the original organization when it comes to handling personal information entrusted to the third party. As a condition of using information from the first organization, the third party agrees to be bound by the first organization's privacy safeguards.

Principle 18 is required by law in Austria, Denmark, France, Sweden, and the United Kingdom, and is part of guidelines drafted by the European Community to apply to all European countries.

Principle 19 is a concept of freedom of information developed by the author. Principle 20 was developed by the author.

Appendix F: Input to this Report

In fulfilling our charge, the task force sought input from many different segments of the academic community. We are grateful for the thoughtful and insightful input we received from each of these sources — administrators, staff, students, and agency and association representatives.

Input from Student Services Administrators and Information Technology Professionals

To better understand the visions, demands, needs, and concerns of the people who traditionally are responsible for collecting, storing, handling, managing, and releasing student information, members of the task force first surveyed the bursars, admissions officers, registrars, and financial aid officers from our own campuses. Additionally, we conducted phone interviews with persons in these same roles on other campuses, asking the following questions:

- What types of records do you maintain and collect?
- What law/policy guides your practices in this area?
- Who are you able to release this information to internally? Externally?
- Where would you like to be in three years regarding electronic handling of data?
- What issues do you see in this regard?

Additionally, the task force solicited input from the CAUSE membership, most of whom are information technology professionals, by requesting contributions of privacy policies, examples of privacy incidents, and identification of key issues.

Individuals from each of the following institutions provided information, responses, and/or comments to members of the task force either in person, via telephone, or via electronic mail. While they did not intend to represent the official position of their institutions, they provided invaluable insight into the dilemmas they face, the questions and concerns they have, and the pressing issues and problems to be resolved.

Arizona State University
Boston College
Brown University
California Lutheran University
California State University System
Carnegie Mellon University
Central Washington University
Central College (Iowa)
Columbia University
Cornell University
Dickinson College
Harvard University
Indiana University
Johns Hopkins University
Lansing Community College
Maricopa Community Colleges
McMaster University
Massachusetts Institute of Technology
Mt. Hood Community College
Northwestern University
Pennsylvania State University
Portland State University
Princeton University
San Diego State University
Seminole Community College
St. Louis University
Simon Fraser University
Sonoma State University
Tufts University
University of Connecticut
University of Delaware
University of Kansas
University of Maryland/College Park
University of Michigan/Ann Arbor
University of New Mexico
University of North Carolina/Chapel Hill
University of Oregon
University of the South
University of Santa Cruz
University of Southern California
University of Tennessee/Knoxville
University of Texas/Austin
University of Virginia
University of Wisconsin/Madison
West Virginia University

Survey of Student Attitudes

Members of the task force also gathered information and comments about electronic access to private and public personal information from students. The task force conducted informal surveys, collecting informal, non-random data from students at the University of Michigan, Pennsylvania State University, the University of the South, the University of Texas at Austin, Indiana University, and MIT. These were not intended to be statistically significant or controlled research studies by any means; however, they did provide anecdotal information regarding some student attitudes and concerns.

Students were asked to rank their preferences on how strongly they felt certain information should be protected, or if it was free to be published within the institution and beyond. The student information types varied from directory information to more personal information.

In general, students felt it was permissible for information traditionally defined as directory information under FERPA (name, address, phone number) to be published within and beyond their institution, such as to other colleges and universities, but not to the general public. A small minority felt this information should be accessible only to others within their institutions. Generally, students felt it was inappropriate for permanent addresses and phone numbers to be published, preferring that only their school addresses be published.

Regarding more personal information, most students were in favor of protecting these records from anyone other than those officials authorized to access the data and the students themselves for review of the files. This view was held whether the frame of reference was within the university, beyond the university to other scholars, or to the general public.

A class of MIT students were asked to identify the pros and cons associated with the institution putting student photos on the Web. Students were thoughtful about the issues, identifying both valuable uses and potential misuses. While they recognized the potential benefits to faculty of having access to student photos, they generally felt that the photos should have restricted access within the university community, and that the placement of photos on the network needed to be fully within the decision-making purview of each student.

Reviewers

Our task force asked a number of individuals with specific institutional or organizational perspectives to review this paper and provide input prior to publication. We are grateful to those who responded to our request:

Robert Atwell, President Emeritus
American Council on Education

Wayne Becraft, Executive Director
AACRAO

Herbert Evert, Associate Registrar
University of Wisconsin/Madison

Susan J. Foster, Vice President, Information Technologies
University of Delaware

Robert Gellman, Privacy & Information Policy Consultant

Marjorie Hodges, Policy Advisor
Office of Information Technologies
Cornell University

Steve Jarrell, Executive Director
Administrative Information Services
University of North Carolina/Chapel Hill

Paula T. Kaufman, Dean of Libraries
University of Tennessee/Knoxville

Anne Oribello, Information Security Officer
Brown University

Rodney Petersen, Coordinator, Policy and Planning
Academic Information Technology Services
University of Maryland/College Park

Richard Rainsberger, Registrar
Central College (Iowa)

LeRoy Rooker/Sharon Shirley
Family Policy Compliance Office
Department of Education

Barbara Simons, Chairperson
United States Policy Committee
Association for Computing Machinery

Duane Webster, Executive Director
Association of Research Libraries

Donald J. Wermers, Registrar
University of Wisconsin/Madison

Appendix G: References

Alderman, E., and C. Kennedy. *The Right to Privacy,* New York: Alfred A. Knopf, 1995.

Allmendinger, Susan. "Internet-Worthy: Getting Students Fit for the Road." *CAUSE/EFFECT*, Spring 1995, 56-57.

American Association of Collegiate Registrars and Admissions Officers (AACRAO). *Guidelines for Post Secondary Institutions for Implementation of the Family Educational Rights and Privacy Act of 1974 As Amended.* Washington, D.C.: AACRAO, 1995.

Askins, Peggy C. (ed). *Misrepresentation in the Marketplace and Beyond: Ethics Under Siege*. Washington, D.C.: AACRAO, 1996.

Baase, Sara. *A Gift of Fire: Social, Legal, and Ethical Issues in Computing*. New York: Prentice-Hall, 1996.

Bernbom, Gerald, Mark Bruhn, and Dennis Cromwell. "Security in a Client/Server Environment." *CAUSE/EFFECT,* Winter 1994, 19-26.

Branscomb, Anne Wells. *Who Owns Information? From Privacy to Public Access*. New York: Basic Books, 1994.

Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. §552a(o) (1988).

Computerization and Controversy: Value Conflict and Social Choices. Edited by Charles Dunlop and Rob Kling. Boston: Academic Press, 1991.

Computers, Ethics & Social Values. Edited by Deborah G. Johnson and Helen Nissenbaum. Englewood Cliffs, N.J.: Prentice-Hall, 1995.

Electronic Communication Privacy Act of 1968, codified as amended at 18 U.S.C. §§2510-21 (1988).

Electronic Privacy Information Center. "Privacy Guidelines for the National Information Infrastructure: A Review of the Proposed Principles of the Privacy Working Group." Report 94-1. In EPIC database [database online]. See http://www.epic.org/privacy/internet/EPIC_NII_privacy.txt

European Parliament and Council of the European Union. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*. Brussels, 1995.

Family Educational Rights and Privacy Act of 1974, 20 U.S.C. §1232g (1996).

Graves, William H., Carol G. Jenkins, and Anne S. Parker. "Development of an Electronic Information Policy Framework." *CAUSE/EFFECT*, Summer 1995, 15-23.

Hodges, Marjorie W., and Steven L. Worona. "Legal Underpinnings for Creating Campus Computer Policy." *CAUSE/EFFECT*, Winter 1996, 5-9.

Information Infrastructure Task Force. Information Policy Committee. Privacy Working Group. "Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information." Final version. June 6, 1995. In EPIC database [database online].

Jacobson, Carl. "Internet Tools Access Administrative Data at the University of Delaware." *CAUSE/EFFECT*, Fall 1995, 7-12.

Johnson, T. "Protecting Privacy in the Face of Technology." *Risk Management* 88 (May 1992).

Johnson, T. Page. "Managing Student Records: The Courts and the Family Educational Rights and Privacy Act of 1974 (FNa)." West Publishing Company, 1993. In Westlaw database [database online], 79 WELR 1, 79 Ed. Law Rep. 1.

Kallman, E., and S. Sherizen. "Privacy Matters." *Computerworld*, 23 November 1992.

Litigation Under the Federal Open Government Laws. 17th ed. Edited by Allan R. Adler. Washington, D.C.: American Civil Liberties Union Foundation, 1992.

Marx, E. "Encrypting Personal Identifiers." *Health Services Research* 29:2 (June 1994).

McLaughlin, J.A. "Intrusions Upon Informational Seclusion in the Computer Age." *John Marshall Law Review* 17:831-839 (1984).

National Research Council Computer Science and Telecommunications Board. *For The Record: Protecting Electronic Health Information*. Washington, D.C.: National Research Council, 1997.

Organisation for Economic Co-operation and Development. "OECD Recommendation Concerning and Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data." O.E.C.D Document C(80)58 (Final). 1980. In EPIC database [database online]. Available on the Internet at http://cpsr.org/cpsr/privacy/privacy_international/international_laws/ 1980_oecd_privacy_guidelines.txt

Porter, John D., and John J. Rome. "Lessons Learned from a Successful Data Warehouse Implementation." *CAUSE/EFFECT*, Winter 1995, 43-50.

Privacy Act of 1974, 5 U.S.C. §552a (1996).

Privacy Rights Clearinghouse. *First Annual Report of Privacy Rights Clearing house*. San Diego, California: Center for Public Interest Law, University of San Diego, 1994.

Privacy Rights Clearinghouse. *Second Annual Report of Privacy Rights Clearing house*. San Diego, California: Center for Public Interest Law, University of San Diego, 1995.

Rainsberger, Richard. *FERPA and Secondary Education: The Family Educational Rights and Privacy Act of 1974 as Amended and the Student*. Washington, D.C.: AACRAO, 1997.

Rezmierski, Virginia. "Electronic Communication: Vapor or Paper?" In *The Use and Abuse of Computer Networks: Ethical, Legal, and Technological Aspects*. Preliminary report based on a conference held December 17 to 19, 1993, at the Arnold and Mabel Beckman Center of the National Academies of Sciences and Engineering, Irvine, California. Washington, D.C.: American Association for the Advancement of Science, 1994.

_____. "Managing Information Technology Issues of Ethics and Values: Awareness, Ownership, and Values Clarification. *CAUSE/EFFECT*, Fall 1992, 12-19.

Smith, H. Jeff. *Managing Privacy: Information Technology and Corporate America*. Chapel Hill, N.C.: University of North Carolina Press, 1994.

Smith, Robert Ellis. *Compilation of State and Federal Privacy Laws*. 1992 ed. Providence, R.I.: *Privacy Journal*, 1992.

U.S. Department of Commerce. "Privacy and the NII: Safeguarding Telecommunications-Related Personal Information." Washington, D.C., 1995. In United States National Information Infrastructure Virtual Library [database online]. Available on the Internet at gopher://www.ntia.doc.gov:70/H0/policy/privwhitepaper.html.

U.S. Department of Education. *Education Data Confidentiality: Two Studies*. Washington, D.C.: U.S. Government Printing Office, 1994.

U.S. Department of Health, Education, and Welfare. Office of Technology Assessment. "Protecting Privacy in Computerized Medical Information." Washington, D.C.: U.S. Government Printing Office, 1973.

U. S. Privacy Protection Study Commission. "Personal Privacy in an Information Society." Washington, D.C.: U.S. Government Printing Office, 1977.

Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy." *The Harvard Law Review*. 4, no. 5 (December 15, 1890): 193-220.

Webster, Sally, and Frank Connolly, "When Bad Things Happen to Good Campuses," *CAUSE/EFFEC*T, Spring 1996, 44-48.

Westin, Alan F. *Privacy and Freedom*. New York: Athenium, 1967.

Appendix H: Resources

AACRAO

The American Association of Collegiate Registrars and Admissions Officers (AACRAO) is a nonprofit, voluntary professional association of more than 8,800 higher education administrators who represent more than 2,300 institutions and agencies in the United States and abroad. AACRAO's *Guidelines for Postsecondary Institutions for Implementation of the Family Educational Rights and Privacy Act of 1974 as Amended* (Richard A. Rainsberger, et al.; 1995; 124 pp; Item #1246) updates current terminology, requirements, procedures, and strategies for compliance, issues such as SPEEDE/ExPRESS, fax, and parental access, student directories, and annual notification of students. The AACRAO Government Relations Department offers a weekly electronic newsletter through the Govrel-L listserv that contains timely information on important subjects, including FERPA and privacy issues. AACRAO's Web site can be found at http://www.aacrao.com/

CAUSE

CAUSE serves as a clearinghouse for information on managing and using information resources in higher education. Its Information Resources Library is an international repository for documents contributed by member campuses, *CAUSE/EFFECT* journal articles, and conference papers. Information about and access to the library is available through the CAUSE Web server (http://www.cause.org/).

Also at the CAUSE Web site is a resource page that provides links to networked information policies that have been contributed to the library, many of which are available electronically on the Web and linked from that page. The page (at http://www.cause.org/issues/policy.html) provides links to related resources, such as the Electronic Frontier Foundation's guidelines for computing policies.

Among the resources listed on the CAUSE policy page is a site at the University of Texas/Austin, developed as part of the task force's efforts, which provides an index and hypertext links to nearly 100 policies that deal with privacy and the handling of student information at various colleges and universities, indexed by state location (see http://www.utexas.edu/computer/vcl/projects/privacy.html).

Computer Security Institute

This membership organization, located in San Francisco, publishes materials and sponsors workshops on the latest in computer security hardware and policies. For further information, call 415-905-2626 or send e-mail to 71702.402@compuserve.com

Electronic Frontier Foundation (EFF)

The Electronic Frontier Foundation is a non-profit civil liberties organization working in the public interest to protect privacy, free expression, and access to public resources and information in new media. EFF's Web site, at http://www2.eff.org, provides a wealth of information related to this subject.

Electronic Privacy Information Center

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC's Web site (at http://www.epic.org) provides legislative updates on these issues and more.

Privacy Journal

Privacy Journal is an independent monthly publication on privacy in a computer age available on a subscription basis. Other privacy-related publications are offered through the journal. Inquire at P. O. Box 28577, Providence, RI 02908 (e-mail 0005101719@mcimail.com).

U. S. Department of Education, Family Policy Compliance Office

This government office enforces the requirements of the Family Educational Rights and Privacy Act and can clarify its requirements. For further information, contact LeRoy Rooker in the Family Policy Compliance Office (leroy_rooker@ed.gov).

CAUSE is an international nonprofit association dedicated to enabling the transformational changes occurring in higher education through the effective management and use of information resources — technology, services, and information. Incorporated in 1971, CAUSE serves its membership of over 1,400 campuses and organizations and nearly 4,000 individuals from its headquarters in Boulder, Colorado.

CAUSE is an Equal Opportunity Employer and is dedicated to a policy that fosters mutual respect and equality for all persons. The association will take affirmative action to ensure that it does not discriminate on the basis of age, color, religion, creed, disability, marital status, veteran status, national origin, race, sex, or sexual orientation, and encourages members and other participants in CAUSE-related activities to respect this policy.