

Executive Summary

The most visible result of the passage of the USA PATRIOT of 2001 (Act) on the University of Wisconsin-Madison campus has been a growing unease among students over their electronic privacy. Students are unclear of what the Act means to their email, library searches, and Internet histories. The University has been less than helpful in the face of this legal sea-change; their electronic privacy policy remains vague and uninformative.

The Act gives federal law enforcement an expanded set of legal tools to obtain electronic information. Bench warrants to capture data transmissions are sufficient where court orders were once required. Suspected terrorist activity gives authorities *carte blanche* to compel production of education and library records. Foreign students suspected of terrorist activity may be surveilled without discernible limits.

While the Act appears to give federal authorities nearly unfettered access to electronic data, it may be a moot point technically. The computer logs that the University's Department of Information Technology keeps on network access are irrelevant from a content perspective. To obtain content, the authorities will have to install their own equipment or use data wiretaps such as the FBI's Carnivore system. Yet, this alone will not -- and should not -- reassure students. The University must educate students on what the law realistically means to their electronic data.

Group Homer recommends:

- The University provides students with a clear and specific electronic privacy statement that references current federal and state privacy and surveillance laws;
- The Department of Information Technology provides easily found links on key homepages to the University's electronic privacy policy;
- The University provides all incoming students with a print version of the electronic privacy policy statement.

Introduction

Recent changes in federal and state privacy and surveillance laws have caused growing concern among University of Wisconsin-Madison students regarding the potential use of their personal information on the University's computer network. Much of this anxiety focuses on the electronic surveillance laws instituted under the USA PATRIOT Act of 2001. The University's response to this legislation was to continue providing students with an ambiguous electronic privacy policy. Combined with the Act's near certain use by federal law enforcement, students concerns about their electronic privacy seem well placed.

Acting on behalf of students, the Associated Students of Madison has requested that Group Homer compile a report that:

- Explains current University/ Department of Information Technology (DoIT) network privacy policies;
- Identifies federal laws, state statutes, and law enforcement policies that effect the use and control of U.S. and international students' electronic information;
- Recommends strategies that the University/ DoIT can use to educate students on laws and policies that effect their electronic information.

University of Wisconsin-Madison Privacy Policies

University of Wisconsin System

The Board of Regents must approve all electronic privacy policies pertaining to University of Wisconsin System institutions. The Board's current policy makes little reference to current federal or state law, except to mention Wisconsin state open-records laws. All other references to privacy are vague and general, such as stating that "no information technology resources can absolutely guarantee the privacy or confidentiality of electronic documents" (University of Wisconsin Regent Policy, p.69).

The policy states that the University will attempt to protect the confidential information of each person. Policy exceptions that dictate who can access confidential information and under what circumstances reflect the exceptions made in federal and state privacy/surveillance laws, which include: 1) to meet the demands of state or federal law; 2) to ensure that data does not destroy institutional property; 3) to "perform routine maintenance and operations" (p.69) and, in the case of file sharing, 4) to ensure individual rights.

Division of Information Technology

The Division of Information Technology's privacy policy adds little more in the way of substance, though enforcement is maintained by a volunteer group of employees called the Badger Incidence Response Team (BadgIRT). BadgIRT manages the University's network logs. Logs contain information such as a specific computer's IP address, date of computer access, length of use, etc. (See Appendix A for an explanation of how log information is generated.) Logs are kept for statistical purposes, and held from a couple of hours to several years, depending upon the volume of logs.

Network logs related to reports of inappropriate use are reviewed by BadgIRT personnel. These logs do not contain enough detailed data to be considered evidentiary. BadgIRT personnel are required to report criminal activity to a law enforcement agency, based on the severity of the activity (Kim Milford, personal communication, September 16, 2003).

Other University Institutions

Currently, University Libraries keep records of patron history (e.g. books checked out, fines owed, etc.) from the computer system's activation in 1999. Library administrators have debated since passage of the PATRIOT Act whether to perform a "patron purge" to eliminate older data (Edith Dixon, personal communication, September 18, 2003). Federal laws do not prohibit libraries from deleting patron files or records, unless it is related to an ongoing law enforcement investigation.

The USA PATRIOT Act and Electronic Privacy

The USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act) introduced a number of legislative changes which significantly increased the surveillance and investigative powers of law enforcement agencies in the United States.

- The Act expands the type of information that an internet service provider must disclose to law enforcement, including records of session times and duration, temporary assigned network addresses, and means or source of payment. Law enforcement officials can now use a subpoena to obtain this information. Under prior laws, officials needed a court order to obtain a user's name, address, telephone toll records, telephone number, and length of service. (Electronic Privacy Information Center, 2003).
- It eliminates the requirement that law enforcement officials provide a person subject to a search warrant with notice at the time of the search. The "secret search" amendment permits seizure of any tangible property or communications when the court finds reasonable necessity. (Electronic Privacy Information Center, 2003).
- Expands the definition of trap and trace devices and pen registers. Previous definitions limited the information that could be collected by these wire-tapping devices to telephone numbers placed from a specific line and the incoming numbers to a specific telephone. New definitions allow for the capture of any electronic data that identifies "the originating number, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication" (Electronic Privacy Information Center, 2003). Obtaining authorization for the use of either wiretap requires a court order but does not require authorities show probable cause.
- The Act required full-implementation of the Student and Exchange Visitor Information System (SEVIS), which was being developed for the Immigration and Naturalization Service (INS) before the September 11 attacks, by January 1, 2003. SEVIS is an Internet-based system that allows schools to transmit student information to the INS for purposes of tracking and monitoring non-immigrant and exchange students (Electronic Privacy Information Center, 2003).
- The Act "permits the FBI to compel production of business records, medical records, education records, and library records without showing a probable cause...." (Electronic Privacy Information Center, 2003). Federal authorities need only claim that the records may be related to an ongoing investigation related to terrorism or intelligence activities.

Several laws limiting law enforcement's ability to intercept citizen's communications, such as Title III, the Electronic Communications Privacy Act (ECPA), and the Foreign Intelligence Surveillance Act (FISA), were substantially amended by the Act.

Foreign Intelligence Surveillance Act (FISA)

The Foreign Intelligence Surveillance Act was passed in 1978 due to "executive branch abuses of electronic surveillance" (Jaeger, 2003, p. 47). The PATRIOT Act amends FISA's requirement that gathering information about foreign intelligence activities must be *the purpose* of the investigation to only being a *significant purpose*.

Electronic Communication Privacy Act

The Act amends ECPA by adding a new voluntary disclosure exception for emergency situations. If an internet service provider, including a university, has reason to believe that an emergency involving immediate danger of death or serious physical injury to any person is imminent, they are justified in disclosing certain information to law enforcement officials (Jaeger, 2003).

Family Educational Rights and Privacy Act (FERPA)

The Family Educational Rights and Privacy Act (FERPA) has two overarching requirements of state-supported educational institutions: 1) students have the right to view their own records, to halt the release of personally identifiable data, and to view the institution's policy on record access; and 2) FERPA prohibits educational institutions from releasing personally identifiable information and records without written consent of the student or their guardian.

FERPA includes several exceptions for the release of student data. Key is the "health and safety" exception which states, "[r]ecords may be released without the student's consent to comply with a judicial order or lawfully issued subpoena and in the case of health and safety emergencies" (Electronic Privacy Information Center, 2003).

Federal Law Enforcement/ Intelligence and the USA PATRIOT Act

The PATRIOT Act expanded the surveillance authority held by law enforcement and intelligence gathering agencies. The Central Intelligence Agency (CIA), FBI, National Security Agency (NSA), Secret Service, were given vast new powers to combat foreign or domestic terrorism:

- The U.S. Constitution prohibits the surveillance of American citizens, yet under the PATRIOT Act an American citizen corresponding with a foreigner may be investigated by the NSA (Bamford, 2002, p. 430);
- The Director of the U.S. Secret Service is required to develop and maintain a national electronic surveillance network for the purpose of preventing terrorism;
- All information obtained by electronic surveillance and a physical search must be coordinated with Federal officers to thwart any act of terrorism;
- The CIA must provide assistance to the Attorney General in order to disseminate potential terrorist information effectively and efficiently.

Carnivore

One of the tools used by the FBI in domestic, electronic surveillance is Carnivore. The Carnivore computer system acts as a computer network trap and trace device/pen register, which

“eavesdrops on packets, watch[es] them go by, then saves a copy of the packets it is interested in” (Graham, 2001).

The FBI must go through a process before they can put Carnivore on a network to collect information.

- The FBI is not allowed to put Carnivore on a network unless the Internet Service Provider claims it cannot (or will not) comply with a court order;
- The FBI must prove they have probable cause and clearly specify who the suspect is, what lines or networks will be tapped, and what kind of information is being seized;
- Carnivore can only collect information from the specified email address;
- Carnivore must be renewed every 30 days.

The Patriot Act, the University, and Students

What does all this ultimately mean to the privacy of student’s network information? Simply, students should not expect privacy from law enforcement, not under current law. Should federal authorities suspect that a student is involved with terrorist activity, they may obtain a warrant and/or subpoena to force production of the student’s network log records, educational records, and library records – all without the student’s knowledge. Further, should the University believe that the student is a threat to the health and safety of others, himself or the nation, administrators could provide most of the same materials without federal law enforcement officials requesting it.

If the student is a foreign national -- the population most at risk of being investigated by federal authorities -- he or she may face surveillance by the NSA or Secret Service. These agencies could request the same information, and, in the case of the NSA, set up a wiretap with only the Attorney General’s authorization (Bamford, 2002).

However ease of access does not necessarily equal a breach in electronic privacy. Based on DoIT’s log policy, it is reasonable to conclude that any network records turned over to federal authorities would be worthless to an investigation. It seems much more likely that should the FBI, CIA, Secret Service or NSA target a particular student, they will do so utilizing their own equipment.

Students need to be aware of this possibility, but the University should not be held culpable for advising students on every option available to law enforcement under the PATRIOT Act. Nevertheless, the University must have a clear policy on who can receive student’s electronic information and under what circumstances.

Recommendations

There are several options available to the University to educate students about possible surveillance. The University could use a pop-up warning to notify students that they may be monitored when logging into the network. This was not recommended as there is no actual monitoring going on at any time. BadgIRT deals with log sheets and statistics, and does not deal with email content. A warning box would be inaccurate, and likely to cause student concern.

Similarly, it is not feasible for the University to place a monitoring warning on the bottom of each University website. This would be even more labor-intensive than the pop-up warning due to the extensive number of websites associated with the University. Moreover, there is no central administrative control over websites, making the placement of such links a logistical impossibility.

Instead, the Homer group recommends the University of Wisconsin implement the following:

- **Privacy Policy Link.** Most students do not have the time to search out the University's privacy policy, and go without understanding what that policy actually says. DoIT could resolve this problem by providing easily found links to the privacy policy at the bottom of each of the following web pages: www.wisc.edu, www.wisc.edu/portal, and <http://my.wisc.edu/portal/index.jsp>.
- **Create a privacy statement with clear and specific details of the UW System and University of Wisconsin-Madison's privacy policy.** Students have a right to know how the "enhanced surveillance powers granted under the Patriot Act and related measures license law enforcement officials to peer into Americans' most private reading, research, and communications" (Kranich, 2003). The Electronic Access Data Policy (written for University faculty, staff, and graduate students) is a detailed and, ultimately, more useful document (see Appendix B), though it, too, could use revision to simplify for student use. Rewriting the University's current policies with that document's detail and the "user friendliness" of the University of Minnesota's online policy (see Appendix C) would help students begin to understand the nature of law enforcement access to their network information.
- **Privacy Policy Pamphlet.** The University should issue a print version of the privacy policy statement with the documents individuals receive when they first enter the University as a student. This help students orient themselves to the privacy environment of the campus before they even step foot on campus.

Sources

- Bamford, J. (2002). *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency*. New York: Anchor Books.
- Electronic Privacy Information Center. (2003, September). *The USA PATRIOT Act*. Retrieved September 17, 2003, from www.epic.org/privacy/terrorism/usapatriot.
- Graham, R. (2001, October). *Carnivore Frequently Asked Questions*. Retrieved September 9, 2003, from <http://www.robertgraham.com/pubs/carnivore-faq.html>.
- Jaeger, P., Bertot, J., & McClure, C. (2003). The Impact of the USA PATRIOT Act on Collection and Analysis of Personal Information Under Foreign Intelligence Surveillance Act. *Government Information Quarterly*. Tallahassee, FL, 2003.
- Kranich, N. (2003, September 15). The Impact of the USA Patriot Act: An Update. *The Free Expression Policy Project*. Retrieved September 17, 2003, from <http://www.fepproject.org/commentaries/patriotactupdate.html>.
- University of Minnesota. (2000). Online Privacy Statement. Retrieved September 17, 2003, from www.privacy.umn.edu.
- University of Wisconsin System Regent Policy Documents. (2003). Madison, WI: UW System Board of Regents.

Appendix A

How network log information is generated.

When connecting to the Internet, a local computer dials into its service provider who then, through the DHCP, lets the computer borrow one of its many IP addresses. The user then wishes to connect to a server holding information (e-mail or a webpage, etc) and so sends a request to that server. The address the user types in is translated into an IP address with the DNS (Domain Name Server) map located at the ISP server the information must pass through (when logging, it is at this point for UW-Madison that IP addresses are saved), the IP address being the location at which the computer acting as the server is residing. Some people may set up a firewall or go through a proxy server to buffer the information flow. A firewall will filter information while a proxy server will save the data in a cache for future access. Cookies are text files created by the site's server for statistical purposes as well as site preferences. This information is stored in name-value pairs, and it usually only holds a unique identifier.

Source: Amy M. Ostrom, personal communication, September 29, 2003.

Appendix B

UW-Madison Electronic Access Data Policy

University of Wisconsin
Madison

Faculty Document 890a
7 October 1991

REPORT OF THE UW-MADISON AD HOC ELECTRONIC DATA ADVISORY COMMITTEE
September 13, 1991 (as revised October 7, 1991 by the Faculty Senate)

INTRODUCTION

The Electronic Data Advisory Committee was created by the University Committee to clarify the privacy and confidentiality status of electronic data and to draft procedures for the University to follow in providing access to information in this form.

The faculty and staff of the University should be under no delusions as to the essential confidentiality of their electronic files. Even when one takes elaborate precautions (e.g. file encryption) the nature of modern communication networks is such that true confidentiality is impossible to guarantee. In addition, the Wisconsin open records law may require public disclosure of electronic data. All users of these services should be apprised of these facts.

The Federal Electronic Communications Privacy Act of 1986 (18 U.S.C. sec. 2511) and parallel language adopted by the Wisconsin Legislature (sec. 968.31(2), Wis. Stats.) allows the University to examine electronic information when necessary to protect the rights and property of the University. The proposed procedures provide a mechanism for doing so in a way that respects the rights of individuals involved.

The report that follows deals with the question of appropriate procedures for the University to follow in cases of requests for access to electronic files initiated internally. (Requests for access that originate external to the University will normally arise under circumstances described in Section 6 of these procedures. In such cases, the University will provide notice to the controller and the opportunity to respond, whenever possible.)

In general, all computer and electronic files should be free from access by any but the authorized users of those files. Exceptions to this basic principle shall be kept to a minimum and made only where essential to

1. meet the requirements of the state open records law and other statutory or regulatory requirements;
2. protect the integrity of the University and the rights and property of the State;
3. allow system administrators to perform routine maintenance and respond to emergency situations such as combating "viruses" and the like: and
4. protect the rights of individuals working in collaborative situations where information and files are shared.

Accordingly the Ad Hoc Electronic Data Advisory Committee recommends the following actions:

1. The University should make a special and periodic effort to notify users that:
 - a. Faculty Policies and Procedures include rules governing the privacy of electronic data;
 - b. State or federal regulations may supersede these policies and procedures; and
 - c. electronic communications and data files are not secure from unauthorized access.

2. Because the proposed policy does not address how departments and schools may access students' instructional accounts, departments and schools should codify their procedures for managing and gaining access to such accounts;

3. The Faculty adopts the following policy and procedures to govern access to electronic files controlled by faculty and staff:

POLICY AND PROCEDURES GOVERNING ACCESS TO ELECTRONIC FILES AT THE UNIVERSITY OF WISCONSIN-MADISON

PRINCIPLES:

The procedures are based on three fundamental principles:

1. Intrusion into electronic files requires carefully considered cause;
2. Controllers of files should be notified before accessing their files; and
3. The University has an obligation to protect the integrity of the University, its services, its confidential data, and the rights and property of the State.

DEFINITIONS

As used in these procedures:

1. "Electronic File" encompasses information stored and/or transmitted in electronic form, including but not limited to text, data, sound, graphics, images, and video, irrespective of its recording and transmission media or its format.

Examples of electronic files include e-mail messages, databases, and magnetic tape files and subsets thereof.

2. "Controller of a file" is defined as follows:

- a. on a single user computer under the control of a single person (e.g., a computer in a faculty office) the files normally are controlled by that person;
- b. on computers accessed by more than one individual, but which do not have an operating system that identifies files with a specific user, the individual responsible to the University for control of the computer (e.g., the laboratory director or department chair) is considered to be the controller of electronic files resident on that computer;
- c. On multiuser systems, an individual is typically registered or given an account. The registered user or account holder is normally considered to be the controller of files held in that account;
- d. In "work for hire" situations where one party enters or edits material for the originator of a file, the one responsible for originating the material in the file is the controller of the file. The person charged with entering the material is usually considered to be an authorized user. For example, when a secretary or a research assistant working under explicit directions uses a computer to enter and edit a document for a faculty member, the faculty member is the controller of the file and the secretary or research assistant is an authorized user.

3. "Authorized User" includes the controller of a file and someone who is given explicit access to the file by a controller.

4. "System Administrator" is an individual who has been charged by a University unit with maintaining a computer system and its software at an acceptable level of performance for the service that it is expected to provide.

PROCEDURES

1. Except as provided for in Sections 5 and 6, no one but an authorized user of an electronic file may intentionally access that file without receiving either

a. The permission of the controller of the file; or

b. The express written permission of the Vice Chancellor for Academic Affairs, who may grant such permission only in accordance with the procedures established by Sections 2 and 3 below.

2. Except as provided for in Sections 5 and 6, the Vice Chancellor for Academic Affairs may grant permission to those persons listed in section 2(b) to access a computer or electronic file only upon determining that the all of the following steps have been taken:

a. The Vice Chancellor for Academic Affairs has received in writing a request for access that specifies the reasons for the requested access and lists the requested file(s) by name, contents, or a description that clearly limits access to the file(s) necessary to further the purposes designated in Section 2(f).

b. The written request has been made by a dean, director, department chair, vice-chancellor, or other person who has responsibility for protecting the integrity of the University, its services, and the rights and property of the State.

c. The Vice Chancellor for Academic Affairs has notified in writing the controller of the file(s) that a request for access to the specified file(s) has been made and is pending. When there is doubt as to who is the controller of a file, notice should be sent to all the known individuals likely to have such an interest.

Notification must, at a minimum,

i. specify the name of the party requesting the file(s);

ii. list by name, description, or contents the file(s) requested;

iii. indicate that unless waived in writing by the controller of the file(s) within four days of notification, an inquiry as specified in section 2(d) of these procedures will be held to examine whether justification exists for granting the requested access;

iv. indicate that in the event a section 2(d) committee has been appointed, the controller of the file(s) has a right to make known to the committee his or her views on whether access is justified;

v. indicate that the file(s) in question shall not be altered or deleted by anyone, including the controller and that alterations or deletions may be a basis for disciplinary action; and,

vi. if relevant, indicate that the Vice Chancellor for Academic Affairs has exercised his or her power under section 3 to take the minimum steps necessary to preserve the contents of the subject file(s).

d. The Vice Chancellor for Academic Affairs has appointed a committee of three members, all of whom are otherwise uninvolved in the request and at least two of whom are members of the faculty or academic staff (as is appropriate to the case), to inquire into whether a justification under section 2(f) exists to warrant granting the requested access. Unless granted additional time, the committee will conduct its inquiry and make a written report to the Vice Chancellor within ten calendar days of its appointment.

At a minimum, the committee shall

i. examine the written request for access provided to the Vice Chancellor under Section 2(a); and

ii. offer all those notified under Section 2(c) an opportunity to make known to the ad hoc committee their views on whether access is justified.

e. The Vice Chancellor for Academic Affairs has received the results of the inquiry specified in Section 2(d) of these procedures or has received the controller's waiver of the section 2(d) inquiry.

f. The Vice Chancellor for Academic Affairs finds that the requested access is necessary to protect the integrity of the University, its services, and the rights and property of the State.

g. The Vice Chancellor for Academic Affairs has put in writing, with as much specificity as possible, the reasons for granting access to the file(s).

3. Upon the written request of one of those persons listed in section 2(b) or on his or her own initiative, the Vice Chancellor for Academic Affairs may authorize the appropriate University unit to take all necessary steps to preserve and save the contents of any file(s) within the University's computer systems. An order to preserve the contents of the file is meant to assure that the data in the file(s) is not destroyed, altered, or lost. Any such order

does not constitute permission to open, read, or otherwise use the contents of the file(s). Access to the contents of the file(s) shall be obtained only under procedures specified herein or under conditions stated in Sections 5 and 6.

4. All requests for access to electronic files made under the Wisconsin open records law shall be made through the office of the University's Custodian of Records. It is recommended that the office of the Custodian of Records promulgate procedures consistent with the Wisconsin open records law and the principles expressed in these procedures. Such procedures shall provide for notice to the controller before public disclosure, whenever possible.

5. Nothing in these procedures is meant

a. to supersede the usual procedures followed by departments and schools in monitoring student accounts given for specific course work; or

b. to preclude computer system administrators from authorizing the routine maintenance of campus computer or communication systems or the rectification of emergency situations that threaten the integrity of campus computer or communication systems, provided that use of accessed files is limited solely to maintaining or safeguarding the system (which may include safeguarding the system from illegal use) or solving specific problems.

6. Nothing in these procedures is meant to either limit or expand access to files pursuant to Wisconsin or United States statutes or regulations, such as those governing patient records, student information files, open records, criminal investigations conducted by federal, state or local law enforcement authorities or certain personnel actions.

The Ad Hoc Electronic Data Advisory Committee:

Seymour Parter, Professor, Computer Sciences and Mathematics (Chair)

David Brown, Senior Policy and Planning Analyst, Office of Information Technology

Dennis Fryback, Professor, Industrial Engineering and Preventive Medicine

Thomas Palay, Professor, Law

Tad Pinkerton, Professor, Computer Sciences & Director, Information Technology

Charlene Rieck, Information Processing Consultant, College of Agricultural & Life Sciences

Source: *University of Wisconsin System Regent Policy Documents*. (2003).

Appendix C

University of Minnesota Online Privacy Statement

The policy of the University of Minnesota is to respect the privacy of all web site visitors to the extent permitted by law. This online privacy statement is intended to inform you of the ways in which this web site collects information, the uses to which that information will be put, and the ways in which we will protect any information you choose to provide us.

There are four types of information that this site may collect during your visit: network traffic logs, web visit logs, cookies, and information voluntarily provided by you.

Network Traffic Logs

In the course of ensuring network security and consistent service for all users, the University employs software programs to do such things as monitor network traffic, identify unauthorized access or access to nonpublic information, detect computer viruses and other software that might damage University computers or the network, and monitor and tune the performance of the University network. In the course of such monitoring, these programs may detect such information as e-mail headers, addresses from network packets, and other information. Information from these activities is used only for the purpose of maintaining the security and performance of the University's networks and computer systems. Personally identifiable information from these activities is not released to external parties without your consent unless required by law.

Web Visit Logs

University web sites routinely collect and store information from online visitors to help manage those sites and improve service. This information includes the pages visited on the site, the date and time of the visit, the internet address (URL or IP address) of the referring site, the domain name and IP address from which the access occurred, the version of browser used, the capabilities of the browser, and search terms used on our search engines. This site makes no attempt to identify individual visitors from this information: any personally identifiable information is not released to external parties without your consent unless required by law.

Cookies

Cookies are pieces of information stored by your web browser on behalf of a web site and returned to the web site on request. This site may use cookies for two purposes: to carry data about your current session at the site from one web page to the next, and to identify you to the site between visits. If you prefer not to receive cookies, you may turn them off in your browser, or may set your browser to ask you before accepting a new cookie. Some pages may not function properly if the cookies are turned off. Unless otherwise notified on this site, we will not store data, other than for these two purposes, in cookies. Cookies remain on your computer, and accordingly we neither store cookies on our computers nor forward them to any external parties. Unless otherwise notified on this site, we do not use cookies to track your movement among different web sites and do not exchange cookies with other entities.

Information Voluntarily Provided by You

In the course of using this web site, you may choose to provide us with information to help us serve your needs. For example, you may send us electronic mail (through a mailer or a web form) to request information, you may sign up for a mailing list, or you may send us your address so we may send you an application or other material. Any personally identifiable information you send us will be used only for the purpose indicated. Requests for information will be directed to the appropriate staff to respond to the request, and may be recorded to help us update our site to better respond to similar requests. We will not sell, exchange or otherwise distribute your personally identifiable information without your consent, except to the extent required by law. We do not retain the information longer than necessary for normal operations. Each web page requesting information discloses the purpose of that information. If you do not wish to have the information used in that manner, you are not required to provide it. Please contact the

person listed on the specific page, or listed below, with questions or concerns on the use of personally identifiable information.

University web sites provide links to other World Wide Web sites or resources. We do not control these sites and resources, do not endorse them, and are not responsible for their availability, content, or delivery of services. In particular, external sites are not bound by the University's online privacy policy; they may have their own policies or none at all. Often you can tell you are leaving a University web site by noting the URL of the destination site.

If you have questions about general University of Minnesota security measures see the University policy, [Collecting Information From Visitors To University Web Sites](#).

If you have questions about this site, its collection of information, and its online privacy statement, contact the site administrator or these [U-Wide numbers](#).

Effective: February 2000

Source: University of Minnesota. (2000).