Report of the SOPAG Privacy Task Force

The SOPAG Privacy Task Force was charged to develop "… a model policy on privacy for library-provided digital services and to recommend practices to enable the policy. The task force will investigate the legal and policy context of online privacy, drawing from Federal and State law, policies of the American Library Association, relevant University of California policies, current campus library patron privacy policies, and other resources that are deemed useful in this endeavor."

During the time period from April to August, 2001, the task force met regularly through conference calls to investigate the elements of privacy in library systems and to create tools to help UC librarians understand how their own systems may impact their ability to provide confidentiality for users of library materials.This report gives the findings of the committee and its recommendations for additional activities to complete the task force's goals.

Members: Karen Coyle (CDL, chair), Sharon Farb (UCLA), Terry Ryan (UCLA), Maryly Snow (UCB), Jacqueline Wilson (UCSF)

Executive Summary

The American Library Association Council adopted a resolution on January 23, 2002, that reaffirms the principles of intellectual freedom in the aftermath of terrorist attacks. The resolution was partly in response to the USA Patriot Act of 2001, HR 3162 RDS. The resolution includes the following:

> "Encourages libraries and their staff to protect the privacy and confidentiality of the people's lawful use of the library, its equipment, and its resources (Policy 52.4, "Policy on Confidentiality of Library Records:)…"

The American Library Association's Office for Intellectual Freedom has also recently released a Draft Interpretation of the Library Bill of Rights on Privacy. In the introduction to this Draft ALA states: "Privacy is essential to the exercise of free speech, free thought, and free association. The courts have upheld the right to privacy based on the Bill of Rights of the U.S. Constitution."

The University of California Libraries now recognize that they need to move from largely informal practices regarding privacy and library systems to a more formal policy. In order to develop a policy recommendation the SOPAG Privacy Task Force investigated applicable federal, and state law as well as UC policies. The Task Force also focused on library information systems and the conflicts they may create for assuring privacy protection. Finally, the Task Force reviewed a wide variety of current university and university library privacy policies and privacy notification styles.

As a result of our review the SOPAG Privacy Task Force recommends:

1. Further development of the draft UC libraries privacy web site created by the Task Force into a UC libraries privacy policy tool.
2. Using the MELVYL-T Catalog as a test case for use of a UC privacy policy tool.
3. Creating a task force to review and propose revision of the University Records Management Disposition Schedule for Library Records.
4. Assigning LTAG or another appropriate group the task of creating guidelines for retention of UC library systems records.
5. Having each UC campus library designate a Privacy Officer to oversee its privacy policies and compliance Areas of Investigation: Law & Policy; Library Systems; Current Practice

Although the charge given to the task force emphasizes the creation of a model policy, it was immediately obvious to the members of the task force that a privacy policy would be an end point, not a starting point. Before developing a privacy policy one has to understand the primary goals of a library in relation to patron privacy and the practical capabilities of the systems that we employ in our institutions.

Law & Policy

In terms of the goals, there were two main areas that needed to be investigated: laws relating to library records (primarily at a state level) and policies of the University. Federal laws relating to privacy may provide background information, but there are no federal laws directly related to library records and privacy.

State Law

Although there is no explicit mention of privacy in our federal constitution, we are fortunate that the California State Constitution does include privacy in its basic rights. We also have a state law pertaining specifically to library records. This is an exception to the California Public Records Act, and exempts from disclosure:

> Library circulation records kept for the purpose of identifying the borrower of items available in libraries, and library and museum materials made or acquired and presented solely for reference or exhibition purposes. The exemption in this subdivision shall not apply to records of fines imposed on the borrowers.

The Public Records Act defines records broadly. Thus, this section may also apply to other kinds of use records such as logs of web use, viewing of library-licensed online materials, or online catalog use.

The Information Practices Act of 1977 recognizes that there is a general danger to privacy in the "indiscriminate" gathering of personal information, and cautions that

> "… In order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits."

This may inform library decisions to keep only that information necessary to perform the information services of the institution.

Policies

The University of California has a rich body of policies relating to public records, to computing and systems, and to student and staff records.

There are two UC policies that specifically pertain to records retention, disposition and use of library records. The UC Records Management Disposition Schedules (Library Records) provides guidelines for the retention and disposition of various types of library records including, but not limited to "circulation records", "borrower records", "interlibrary loan requests" etc. UC Policy Business and Finance Bulletin RMP-1, University Records Management Program outlines the scope, definitions and records disposition schedules which are mandatory and apply to all units within the University. UC Policy Business and Finance Bulletin RMP-1 defines a record as:

> "**Record:** the written, visual or audio documentation of any action or activity generated or received by an operating unit of the University. Records may include correspondence, other types

> of papers, cards, forms, maps, tapes, magnetic tapes, films, prints, exhibits, catalogues, pamphlets, etc. (See statement on University ownership of administrative records in Business and Finance Bulletin RMP-1.)"

The University Records Management Program Disposition Schedules are periodically reviewed and revised and are currently scheduled for a major overhaul. According to RMP-1, "[a]ny staff member may secure a copy of Form RM-2 from a Records Management Coordinator and initiate a disposition schedule review. (See Section V., below.) All requests for establishment of disposition schedules will be reviewed by the University Records Management Committee for legal, audit, and archival value. RMP-1 Section V. A. states that "[w]ithin each office or department one individual should be assigned the responsibility to monitor the records disposition program for that unit." In addition, "[t]o assure that records of historical value are not destroyed, each "Request for Establishment of Record Disposition Schedule" (form RM-2) is reviewed by the appropriate University Archivist on each campus before it is submitted to the Records Management Committee" thereby providing the University Libraries with an additional level of review and input on record disposition schedules.

The UC Electronics Communications Policy (UC ECP) revised and reissued in November 2000, states is scope and purpose as follows:

> "Recognizing the convergence of technologies based on voice, video, and data networks, this Policy establishes an overall policy framework for electronic communications. This Policy establishes new policy and procedures where existing policies do not specifically address issues particular to the use of electronic communications."

Section IV A. specifically addresses the University's committee to privacy as follows:

> "The University recognizes that principles of academic freedom and shared governance, freedom of speech, and privacy hold important implications for the use of electronic communications. This Policy reflects these firmly-held principles within the context of the University's legal and other obligations. The University respects the privacy of electronic communications in the same way that it respects the privacy of paper correspondence and telephone conversations, while seeking to ensure that University administrative records are accessible for the conduct of the University's business. "

In addition, University policy (see Business and Finance Bulletin RMP-8) prohibits University employees and others from "seeking out, using, or disclosing" personal information without authorization, and requires employees to take necessary precautions to protect the confidentiality of personal information encountered in the performance of their duties or otherwise. This prohibition applies to electronic communications. In this Policy the terms "inspect, monitor, or disclose" are used within the meaning of "seek, use, or disclose" as defined in RMP-8.

The UC Electronics Communications Policy can be found on the web at:
http://www.ucop.edu/ucophome/policies/ec/html/welcome.htm

The UC Policy Business and Finance Bulletin Legal Requirements on Privacy of and Access to Information RMP-8 can be found on the web at: http://www.ucop.edu/ucophome/policies/bfb/rmp8toc.html

The UC Records Management Deposition Schedules can be found on the web at:
http://www.abs.uci.edu/depts/mailrec/uci-ppm/procs/700/viii.html

UC Business and Finance Bulletin RMP-2, Records Disposition Program and Procedures can be found on the web at: http://www.ucop.edu:80/ucophome/policies/bfb/rmp2a.html

In addition to the above mentioned federal and state law and UC policies pertaining to privacy and library information communication and technology there are a number of additional statutes and policies that specifically protect confidential student as well as faculty and staff information. From the outset, The Privacy Task Force focused on the range of issues specifically relevant to libraries and privacy in the online environment rather than the larger issues related to online privacy and the University including employment and student records. Additional federal, state and UC policies should be consulted regarding these broader issues.

Library Systems

Protecting the privacy of our users is both a professional value of librarianship and a requirement by law and policy. Protecting privacy in information systems is challenging, though, because of legitimate needs that can conflict with complete privacy protection. Some of the goals that may seem in conflict with privacy protection include:

- Providing customized services to our users. In order to provide tailored services, we need to keep information about our users and be able to access it easily whenever they connect to our systems.
- Tracking statistics and management information to assess and improve our service. We can make better decisions when we have detailed information about who are using our collections and services.
- Monitoring system use to detect intrusions and abuse. The Information Superhighway has become a mean street, and responsible systems managers must keep a wary eye on system use for signs of unauthorized intrusion and abuse.
- Identifying those who have used systems for illegal or harmful purposes. When our systems are used inappropriately, there is great pressure to identify those responsible, from management and from law enforcement.
- Running systems in an efficient and cost-effective manner. Many systems we install come set up to collect a lot of personal information from users. Turning off such practices or adding specialized routines to protect privacy can be costly.

Thoughtful privacy practices can meet these goals without compromising our ethical and legal obligation to protect the privacy of library users, by adhering to the following basic principles:

- Know what information your systems are collecting that match identity with information seeking behavior.
- Keep the minimum information necessary to meet your legitimate goals, and don't collect information "just in case."
- Keep the information only as long as you must.
- Restrict access to the information to those who need to use it in the normal course of Library business and reveal it to third parties only with appropriate authority.
- Tell your users what information you are keeping and why, and how to ask you for more clarification.
- Be particularly careful of information about users with very rigorous legal protections, such as students and patients.

Current Practice in Library Privacy Notification

The task force investigation included a study of privacy notices on library-related web site. In 2001, a wide variety of university and university library privacy notification styles can be found on the Internet. This variety refers to both depth and breadth of information on privacy as well as the location, or multiplicity of locations, of privacy policies. While the majority of institutions of higher education and their libraries have not displayed their privacy policies on the web, a growing number are choosing to prominently display

privacy statements. These policy statements range from the very brief to exhaustive, multi-page descriptions. Because an institution of higher education may have hundreds of web pages, the posting of a privacy policy at its portal or gateway page could easily be overlooked. A small number of institutions have begun posting privacy policies on multiple web pages. The usual locations for privacy policies is the portal or gateway page and the main library page. However, because many Internet users go directly to specific library web pages, they may easily miss seeing any privacy policy statements.

The contents, or elements, of privacy policies range in depth but generally cover who, what, when, where, and why. (For further information, see http://www.slp.ucop.edu/sopag/privacytf/elements.html.)

- who collects user information and who has access to it
- what information is collected
- the duration for which the information is retained
- when the policy was devised and when it might be revised
- where the privacy policy originated and how to contact its originators
- why the information is collected

Privacy policy statements generally address both the "rights of hosts" and the "rights of users",

Privacy policy statements may contain an introductory statement of commitment, including areas of vulnerability such as chat rooms and message boards. The description of why information is collection can include improvement of service, statistical analysis of trends, identification of system performance problem areas, prevention of hacking (denial of service attacks, unauthorized changed information, and hardware damage). A few institutions have stated whether they are using intrusion detection systems, and some even mention which monitoring software they use by name. The type of information collected may include aggregate or individual domain internet service provider URLs of both the user and the pages visited. A particularly important category of information is personally identifiable information. This may include name, address, zip code, email address, birth date, gender, social security number, password. Often the collecting of cookies, persistent or not, is addressed.

Who gets the information may be explicitly spelled out, ranging from which type of authorized person, such as a circulation library assistant) to the institution as a whole, or law enforcement. Some institutions make careful distinction between informal, formal, and legal (subpoenaed) requests from law enforcement.

Many institutions warn visitors that following links will lead the visitor away from the host site into areas where privacy is not protected. Again, chat rooms and message boards are frequently cited.

A few institutions suggest to the viewer that they revisit the privacy policy page again in a specific period of time, often 3 months or 6 months, as the policy might change. A few also define terms such as "personally identifiable information", "cookies", "persistent cookies". Some institutions show the user an actual example of the information returned to the computer when a web page is accessed. Links for contacting the host of the privacy policy are rare, but important.

Recommendations

1. Further Development of Web Site into Privacy Policy Tool

   The task force developed a sketch of a web site that would serve all UC librarians in the understanding and development of privacy policies. (See http://www.slp.ucop.edu/sopag/privacytf/mockup.html). This web site needs to be developed into an easy to navigate site with a consistent interface. The temporary version of this site is housed on the CDL Libstaff website. We need to find an appropriate permanent home for this site and staff

that will enhance and maintain it. The web site, when completed, should serve as a "how to" that helps libraries through the steps of defining their privacy policy, performing an audit of their library systems, and posting the privacy policy on the library web pages.

2. Use of MELVYL-T as a Test Case

   The development of the Union Catalog on a new technology platform is an opportunity to test some of the principles in this document. The Union Catalog is a subset of a library ILS containing OPAC functionality but not other systems such as circulation and patron files. Decisions have to be made in any case on the storage of activity logs and the protection of patron profiles; user privacy decisions could be made at the same time. The CDL could report on its experience in terms of the feasibility of implementation of the goals in this document.

3. Review and Revision of University Records Management Disposition Schedule for Library Records

   Records retention and disposition schedules are a necessary component of any records management system. In an increasing online environment, the definitions, scope and identification of relevant records is essential. The current disposition of library records has not been reviewed for a decade. SOPAG should appoint a task force to review and propose recommendations for revision of the disposition of library records in light of the current legislation and findings of the Privacy Task Force.

4. Determination of Library Systems Standards

   It would save the UC libraries considerable time if we could have some general standards or guidelines for which library systems records should be stored beyond their immediate use and for how long. The appropriate group to determine if general guidelines are feasible, and to develop them if they are, is probably LTAG.

5. Designation of a Privacy Officer at Each Institution

   Each UC library needs to have at least one staff member who has the responsibility to oversee that institution's privacy policies and compliance. This may be a staff member who already has general policy responsibility for the institution. This person should also be tasked with keeping up with the ever-changing privacy environment as it affects libraries and library records, and with overseeing staff education in this area.