SOPAG Privacy Task Force
Privacy Audit and Guidelines
DRAFT 8/13/01

This guide to conducting a technology privacy audit is designed to alert you to system locations where private information is likely to exist, and to suggest actions to take to protect that information. 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 is 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.

Library Application Systems | Library Server Logs | Library Public Workstations | Network Services | Licensed Services

Location of Private Information	Minimum Practices to Meet Legal or Policy Requirements	Additional Practices to Consider	Relevant Legislation and Professional Codes
Library Application Systems (Integrated Library Systems, Electronic Reserves, Electronic Reference, Staff Directories, etc.)			
Circulation and borrower records, including: • Patron registration records[1] • Circulation transaction logs • Overdue and billing records • Records of paging from RLFs and local storage • Document delivery & interlibrary loan transactions • Records of access to electronic reserves	Restrict access to records and logs that reveal what was borrowed by a patron, as well as to patron registration records, to library staff who have a legitimate need to see the records. Don't allow access to records or logs that reveal what was borrowed, or to patron registration records, to non-library personnel without proper written authorization from the patron or by court order. Delete patron registration records 0-5 years after expiration of borrower privileges. Be aware that the amount of fines or fees owed by a patron may be shared with other campus systems and may be disclosable under the California Public Records Act.	Delete individual identity as soon as possible after a transaction is resolved (that is, when the item has been returned, all bills are paid, etc). For statistical analysis, preserve only the category of user. Keep billing information only as long as required by campus financial record policies. Post on the library Web site what information you keep about patron borrowing histories, how long it is kept, and who can see it. Ca. Government Code Section 6254 (j)	Ca. Government Code Section 6254 (j) [2] Ca. Government Code Section 6267 [3] Ca. Constitution Article 1 [4] ALA Code of Ethics 54.15 pt. 3 [5] SAA Code of Ethics Section IX [6] UC Records Management Disposition Schedules (Library Records) [7] Note: Records of fines are specifically exempt from Ca. Government Code Section 6254(j) and 6267
Records to support personalized services, including: • Search histories saved beyond a session	Notify users in advance whenever personally identifiable information (such as name, user ID, email address, etc) is requested and will be stored on the system.	Advise users of the privacy exposures involved in providing information to support personalized services. Offer users the option of more limited	UC Electronics Communications Policy (UC ECP) Section IV. B.C. [8] Family Educational Rights and

• Saved searches and sets • SDI profiles • Files/logs of previous electronic reference queries and answers	Restrict access to personally identifiable records to library staff who have a legitimate need to consult. Don't provide personally identifiable records to a third party without the explicit permission of the patron, pursuant to the UC ECP or by court order.	services, without the need to provide personal information Regularly purge unused records with personally identifiable information. If reference answers are kept in a "knowledge bank" for re-use, delete information on the asker before saving.	Privacy Act of 1974 (FERPA) 20 USC 1232g [10] Ca. Information Practices Act. Ca. Civil Code Section 1798 et seq. [11] Ca. Government Code Section 11015.5 [12] ALA Code of Ethics Section III [13]
OPAC search logs (see also Web server logs below)	Restrict access to search logs to library staff who have a legitimate need to see the records. If individual identity is logged, have an online notice advising users that such records exist and privacy can't be guaranteed.	Log only aggregate information about users if possible. If individual identity is logged, delete individual information as soon as possible, keeping searching information by category of user only for statistical analysis.	ALA Access to Electronic Information, Services and Networks: An Interpretation of the Library Bill of Rights.
Online displays of patron borrower records, patron-initiated renewals, and the like via the OPAC	Allow access to a patron's borrowing record only to the patron.	For students, don't display any personal information that is not defined as "directory information" on your campus under FERPA. Time out displays of patron information. Advise patrons to close session before leaving shared machines such as library public stations, lab machines, etc. Disable ability to use the browser back	Ca. Government Code Section 6254 (j) [2] Ca. Government Code Section 6267 [3] Ca. Constitution Article 1 [4] ALA Code of Ethics 54.15 pt. 3 [5]

		button to re-display patron borrower screens Allow patrons to "opt out" of having their borrowing record display via the OPAC.	FERPA 20 USC 1232g [10] Ca. Information Practices Act. Ca. Civil Code Section 1798 et seq. [11] ALA Code of Ethics Section III [13]
Directory servers that allow user queries	Treat patron directory information with the same restrictions as patron registration records described above. For students, don't display any personal information that is not defined as "directory information" on your campus under FERPA. Block queries about any student who has requested suppression of his/her directory information under FERPA.	Include only library staff information in a library-managed directory server that supports user queries, never include patron records.	FERPA, 20 USC 1232g [10]
Directory servers that allow trusted application queries only	Control access to the directory to trusted applications only Document clearly what information is provided and to whom	Establish written memos of understanding with the systems administrators of any application that will be sending queries, prohibiting them from sharing directory information with third parties. Do not share any student directory information with any application that is not managed within the University of California. Limit the amount of directory information shared with any application.	FERPA, 20 USC 1232g [10]

Location of Private Information	Minimum Practices to Meet Legal or Policy Requirements	Additional Practices to Consider	Relevant Legislation and Professional Codes
Library Server Logs			
Library Web server logs, including proxy servers	If access is authenticated by user ID: Notify users that the user ID will be stored in Web server logs. Restrict access to server logs to library staff who have a legitimate need to consult. Don't provide server logs to a third party without the explicit permission of the user, pursuant to the UC ECP or by court order.	Since the IP addresses that are routinely logged by Web servers can sometimes be used to determine user identity, don't provide server logs to a third party except by court order. Routinely purge log files, keeping only aggregate data for statistics tracking. Publish statistics of Web usage in the aggregate only, without individual IP addresses.	UC Electronics Communications Policy Section IV. B.C. [8] Ca. Government Code Section 11015.5 [12]
Mail message files	Keep files secure and limit access to the message recipients and authorized library systems staff only. Limit inspection of mail message files by systems staff to the minimum needed for proper functioning and security of the system. Get proper authorization from a Vice Chancellor before inspecting any mail message files, or allowing anyone else to inspect mail message files. If the message file includes email from a student, always get advice of counsel as well. Notify the user if any mail message files are inspected. Notify	Advise users to understand the logging practices and policies of any other mail provider used. Purge message files regularly	UC ECP Section IV. B.C. [8] FERPA 20 USC 1232g [10] Ca. Information Practices Act. Ca. Civil Code Section 1798 et seq. [11] Ca. Government Code Section 11015.5 [12]

	before inspection except in emergencies.		
Mail server logs	Keep log files secure and limit access to authorized systems staff only. Log only transactional message header information. Do not routinely trap and log mail messages, engage such logging only if required to investigate a specific incident of abuse. If such logs are to be kept, follow same practices as defined above for mail message files.	Purge logs regularly.	UC Electronics Communications Policy Section IV. B.C. [8]

Location of Private Information	Minimum Practices to Meet Legal or Policy Requirements	Additional Practices to Consider	Relevant Legislation and Professional Codes
Library Public Workstations			
Browser caches, including history files	Keep logs secure and limit access to authorized library systems staff only. Limit inspection of logs by systems staff to the minimum needed for proper functioning and security of the system. Don't provide logs to a third party without the consent of the patron, authorization from a designated Vice Chancellor, or a court order.	Purge all public workstation caches frequently	UC Electronics Communications Policy Section IV. C.(1) c [8] Ca. Government Code Section 11015.5 [12]
Cookies & certificates	Since cookies and certificates often contain personally identifiable information, keep cookie & certificate files secure and limit access to authorized library systems	Advise users of the privacy exposures involved in using cookies	UC Electronics Communications Policy Section IV. C.(1) c [8]

	staff only. Limit inspection of cookies and certificates by systems staff to the minimum needed for proper functioning and security of the system. Don't provide cookie & certificate files to a third party without the consent of the patron, authorization from a designated Vice Chancellor, or a court order.	Advise users to always use password control for personal certificates Purge cookies and certificate files frequently Make cookie file read-only after installing cookies for any content sites of importance	Ca. Government Code Section 11015.5 [12]
Operating system logs	If logs include personal information such as login IDs Keep logs secure and limit access to authorized library systems staff only. Limit inspection of logs by systems staff to the minimum needed for proper functioning and security of the system. Don't provide logs to a third party without the consent of the patron, authorization from a designated Vice Chancellor, or a court order.	Don't log personal information such as individual login IDs, files consulted, and the like unless required to investigate a specific incident of abuse or a specific system problem. Purge logs with personal information frequently. Advise users to inquire about logging and retention policies for shared workstations in other locations	UC Electronics Communications Policy Section IV. B.C. [8]
Browser bookmarks		Allow only systems administrators to create and edit bookmark files, don't store personal bookmarks on public workstations. Advise users to delete personal bookmarks from shared machines in non-Library locations	ALA Code of Ethics 54.15 pt. 3 [5]
Mail message files	If mail messages are stored locally at the public workstation Keep files secure and limit access to authorized library	Disable the ability to save mail messages to public workstation disks, allow only remote storage.	UC ECP Section IV. C.(1) c [8] Ca. Government Code

	systems staff only. Limit inspection of mail messages by systems staff to the minimum needed for proper functioning and security of the system. Get proper authorization from a Vice Chancellor before inspecting any mail messages, or allowing anyone else to inspect mail messages. If the message is from a student, always get advice of counsel as well. Notify the user if any mail messages are inspected. Notify before inspection except in emergencies.	If messages are stored locally, purge the mail message files frequently	Section 11015.5 [12]
Peeping Toms (patron watching what her neighbor is doing)		Install privacy screens Position workstations so screens can't easily be seen from neighboring workstations	
Paper sign-up sheets	Limit review of sign-up sheets to authorized library staff only.	Keep sign up sheets for a limited period of time	ALA Code of Ethics 54.15 pt. 3 [5]

Location of Private Information	Minimum Practices to Meet Legal or Policy Requirements	Additional Practices to Consider	Relevant Legislation and Professional Codes
Network Services			
Router/switch log	Keep any traffic logs secure and limit access to library systems staff.	Though security often requires automated analysis of all network traffic, never record or log that traffic, or create a	

	Limit inspection of logs by systems staff to the minimum needed for proper functioning and security of the system. Don't provide logs to a third party without the consent of the patron, authorization from a designated Vice Chancellor, or a court order.	system that allows human review, unless required to investigate a specific incident of abuse When such logs are created, limit access to Verify that network partners have clear and limited policies for human review of network traffic. Alert users to review the policies of their ISPs to understand what monitoring of network traffic occurs.	

Location of Private Information	Minimum Practices to Meet Legal or Policy Requirements	Additional Practices to Consider	Relevant Legislation and Professional Codes
Licensed Services (Licensed content, outsourced server hosting, campus services, etc)			
Remote Web sites, including Content providers, outsourced Web hosting, proxy servers, etc.		Advise users of limits to library privacy protection when using remote sites. Negotiate for proper and secure logging practices and procedures in contracts	
Personalization profiles (such as PubMed Cubbies) and other service offers for personal information ("give us your email address and we'll notify you of new titles in your area of interest")		Advise users of the privacy exposures involved in providing information to support personalized services. Negotiate for clause in License Agreement regarding confidentiality of user information.	

Usage statistics		Negotiate for clause in License Agreement that provides for confidentiality of individual users and for usage statistics in aggregate	

[1] It should be noted that archival practice and special collection unit practice regarding privacy, confidentiality and retention of user registration records are different from that of libraries. For example, American Library Association/SAA Joint Statement on Access to Original Research Material emphasizes the importance of "confidentiality in its collections" rather than for its users. See Section 2. "A repository is committed to preserving manuscript and archival materials and to making them available for research as soon as possible. At the same time, it is recognized that a repository may have legal and institutional obligations to protect confidentiality in its collections, and that private donors have the right to impose reasonable restrictions upon their papers to protect privacy or confidentiality for a reasonable period of time." Available on the Web at: http://www.ala.org/acrl/guides/ala-saa.html. See also Pugh, M. J. (1992). Providing Reference Service for Archives and Manuscripts. p. 95-96. "The numerous forms and reference letters generated in providing reference services must be filed and appropriate retention periods determined for them. Most forms are retained in case the archives discovers theft, abuse, or misuse. Reference records are also used to support requests for reference tools, equipment, staff and finding aids; such forms provide the basis for user studies. Little guidance has been published on the scheduling and disposition of reference records. Researcher registration records are usually filed by the name of the user in an annual file and kept for as long as possible. Request forms are filed and kept for as long as possible to provide evidence in case of theft or abuse of records. The National Archives keeps both registrations forms and call slips for twenty-five years. Photocopy request forms also are retained because they require a signature by which the user agrees to abide by copyright law. If later publication exceeds fair use, the repository will want to show that it warned the user. One repository keeps all reference letters for five years, filed in annual files, thereunder alphabetically by user. After five years, routine letters are destroyed; significant correspondence is kept indefinitely." As fyi, the UC Records Management Disposition Schedules for authorization cards/library card application info requires that records are destroyed 0-5 years after expiration.

[2] Ca. Gov. Code 6254(j) 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.

[3] Ca. Gov. Code 6267. All registration and circulation records of any library which is in whole or in part supported by public funds shall remain confidential and shall not be disclosed to any person, local agency, or state agency except as follows: (a) By a person acting within the scope of his or her duties within the administration of the library. (b) By a person authorized, in writing, by the individual to whom the records pertain, to inspect the records. (c) By order of the appropriate superior court. As used in this section, the term "registration records" includes any information which a library requires a patron to provide in order to become eligible to borrow books and other materials, and the term "circulation records" includes any information which identifies the patrons borrowing particular books and other material. This section shall not apply to statistical reports of registration and circulation nor to records of fines collected by the library.

[4] California Constitution Article 1 Declaration of Rights. Section 1. All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.

[5] ALA Code of Ethics 54.15 pt. 3. Librarians must protect each user's right to privacy with respect to information sought or received, and to materials consulted, borrowed or acquired;"

[6] SAA Code of Ethics Section IX. Information about Researchers, "Archivists endeavor to inform users of parallel research by others using the same materials, and, if the individuals concerned agree, supply each name to the other party."

[7] UC Records Management Disposition Schedules. Library Records. Available on the web at: http://www.abs.uci.edu/depts/mailrec/uci-ppm/procs/700/viii.html

[8] Available on the Web at: http://www.ucop.edu/ucophome/policies/ec/html/ecppolicy_sectionIV_pivacyandconfidentiality.htm "An electronic communication holder's consent shall be obtained by the University prior to any inspection, monitoring, or disclosure of the contents of University electronic communications records in the holder's possession, except as provided for below. The University shall only permit the inspection, monitoring, or disclosure of electronic communications records without the consent of the holder of such records: (i) when required by and consistent with law; (ii) when there is substantiated reason … to believe that violations of law or of University policies…, have taken place; (iii) when there are compelling circumstances as defined…; or (iv) under time-dependent, critical operational circumstances as defined…."Except when otherwise provided by law, users of University electronic communications systems and services shall be informed whenever personally identifiable information other than transactional information will be collected and stored automatically by the system or service." Transactional information is that "needed either to complete or to identify an electronic communication. Examples include but are not limited to: electronic mail headers, summaries, addresses and addressees; records of telephone calls; and IP address logs." "In no case shall electronic communications that contain personally identifiable information about individuals, including data collected by the use of "cookies" or otherwise automatically gathered, be sold or distributed to third parties without the explicit permission of the individual." "During the performance of their duties, personnel who operate and support electronic communications resources periodically need to monitor transmissions or observe certain transactional information to ensure the proper functioning and security of University electronic communications resources and services. On these and other occasions, systems personnel might observe the contents of electronic communications. Except as provided elsewhere in this Policy or by law, they are not permitted to seek out the contents or transactional information where not germane to the foregoing purposes, or disclose or otherwise use what they have observed. Such unavoidable inspection of electronic communications is limited to the least invasive degree of inspection required to perform such duties. "

[10] Federal Family Educational Rights and Privacy Act of 1974. 20 USC 1232g. Available on the Web at: http://www4.law.cornell.edu/uscode/20/1232g.html "For the purposes of this section the term ''directory information'' relating to a student includes the following: the student's name, address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, and the most recent previous educational agency or institution attended by the student" "Any educational agency or institution making public directory information shall give public notice of the categories of information which it has designated as such information with respect to each student attending the institution or agency and shall allow a reasonable period of time after such notice has been given for a parent to inform the institution or agency that any or all of the information designated should not be released without the parent's prior consent." "No funds shall be made available under any applicable program to any educational agency or institution which has a policy or practice of releasing, or providing access to, any personally identifiable information in education records other than directory information…. unless - (A) there is written consent from the student's parents…or… such information is furnished in compliance with judicial order, or pursuant to any lawfully issued subpoena, upon condition that parents and the students are notified of all such orders or subpoenas in advance of the compliance therewith" "For the purposes of this section, whenever a student has attained eighteen years of age, or is attending an institution of postsecondary education, the permission or consent required of and the rights accorded to the parents of the student shall thereafter only be required of and accorded to the student.

[11] Ca. Information Practices Act. Ca. Civil Code Section 1798 et seq. "The Legislature declares that the right to privacy is a personal and fundamental right protected by Section 1 of Article I of the Constitution of California and by the United States Constitution and that all individuals have a right of privacy in information pertaining to them. The Legislature further makes the following findings: (a) The right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies. (b) The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information. (c) In order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits." Available on the Web at: http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798-1798.1

[12] Ca. Gov. Code § 11015.5, "Electronically collected personal information" means any information that is maintained by an agency that identifies or describes an individual user, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, medical or employment history, password, electronic mail address, and information that reveals any network location or identity, but excludes any information manually submitted to a state agency by a user, whether electronically or in written form, and information on or relating to individuals who are users, serving in a business capacity, including, but not limited to, business owners, officers, or principals of that business.

[13] ALA Code of Ethics Section III. "We protect each library user's right to privacy and confidentiality with respect to information sought received and resources consulted borrowed, acquired or transmitted."

[14] ALA Access to Electronic Information, Services and Networks: An Interpretation of the Library Bill of Rights. "Users have both the right of confidentiality and the right of privacy. The library should uphold these rights by policy, procedure, and practice, users should be advised however, that because security is technically difficult to achieve, electronic transactions and files could become public."