Questions and Answers on Privacy and Confidentiality

The IFC developed this Q&A to work in conjunction with Privacy: An Interpretation of the Library Bill of Rights, adopted by the ALA Council on June 19, 2002. Revised April 14, 2005; June 26, 2006; October 30, 2006; January 23, 2012; July 1, 2014.

In the last decade challenges to privacy from a multitude of sources have been on the rise. Consequently questions about privacy and libraries are escalating. The Privacy Subcommittee of the American Library Association's Intellectual Freedom Committee has prepared this "Q & A" to provide additional guidance for librarians struggling with privacy issues.

I. Basic Concepts—Definitions, Rights, and Responsibilities

1. What is the difference between privacy and confidentiality in a library?

In a library, user privacy is the right to open inquiry without having the subject of one's interest examined or scrutinized by others. Confidentiality exists when a library is in possession of personally identifiable information (see No. 2. "What is personally identifiable information" below) about users and keeps that information private on their behalf. Confidentiality is a library's responsibility. This responsibility is assumed when library procedures create records such as closed-stack call slips, computer sign-up sheets, registration for equipment or facilities, circulation records, what Web sites were visited, reserve notices, or research notes.

In protecting the privacy rights and the confidentiality rights of library users, librarians, staff, educators, volunteers, and trustees should limit the degree to which personally identifiable information is monitored, collected, disclosed, and distributed while fulfilling their duty to comply with their state's library confidentiality statute. Librarians involved in training volunteers, new employees, student assistants, or trustees should inform them of the requirements that they not abuse confidentiality and that they protect library users' rights of privacy.

For ALA's privacy policies and "Privacy: An Interpretation of the Library Bill of Rights," see the *Intellectual Freedom Manual*, (2010), and the Web site, "Privacy and Confidentiality."

2. What is "personally identifiable information", and why is this phrase used?

"Personally identifiable information" (PII) covers a greater range than "personal identification," such as an individual's name, address, telephone number, social security number, driver's license number, e-mail address, etc. PII connects you to what you bought with your credit card, what you checked out with your library card, and what Web sites you visited where you picked up cookies. More than simple identification, PII can build up a picture of your tastes and interests — a dossier of sorts, though crude and often inaccurate. While targeted advertising is the obvious use for PII, some people would use this information to assess your character, decide if you were a security risk, or embarrass you for opposing them. For minors seeking personal, social, and sexual identities, having the subjects of their research or reading known may be embarrassing or put them at risk for teasing or bullying. Because of the chilling effect that such scrutiny can have on open inquiry and freedom of expression, libraries and bookstores have long resisted requests to release information that connects individual persons with specific books.

"Personally identifiable information" has become the generally accepted phrase and has been in use in ALA policy since the 1991 adoption of the "Policy Concerning Confidentiality of Personally Identifiable Information about Library Users."

3. If there is no reasonable expectation of privacy in a public place, how can anyone expect privacy in a library?

A library cannot be responsible for someone being seen or recognized in a library but should take steps to protect user privacy whenever possible. That is, in a library, a user's face may be recognized, but that does not mean that the subject of the user's interest must also be known. The interior design and functions of library buildings — including school libraries — can be planned to preserve privacy of inquiry, even while the user's presence and behavior remain observable. Thus, both safety and privacy are maintained. To the greatest extent possible, the user should be able to work independently, both to afford privacy and to reduce the quantity of confidential records for which the library must be responsible.

4. I know people can be suspicious of what bureaucrats might do with personal information, but I'm a librarian — can't people just trust me?

While we librarians don't often think of ourselves as government bureaucrats, members of the public may see us as authorities just like a uniformed police officer or a robed judge. In fact, staff in publicly funded libraries are part of government and are constrained by all the laws that restrict the power of government. One of the lessons learned on the way to democracy was that no matter how ethical the current office holder may be, someday someone else may try to abuse the position. Laws and institutional policies are among the ways we make sure that we aren't totally dependent on the character of the person in the job. Policies can provide guidance and strength, especially when new technology makes issues look different, By establishing strong privacy and confidentiality policies, libraries and schools can protect staff from pressure to violate users' rights.

5. Why is it important for my library to have a privacy policy, and what should the policy cover?

All libraries — not just those that are publicly funded — should have in place privacy policies and procedures to ensure that confidential information in *all* formats is protected. A privacy policy communicates the library's commitment to protecting user information and helps prevent liability and public relations problems. Librarians should consult with their attorneys or school district legal counsel to develop policies that limit the degree to which personally identifiable information is monitored, collected, retained, disclosed, and distributed.

"Privacy: An Interpretation of the Library Bill of Rights," is intended to reaffirm and clarify the long-standing commitment of librarians to protect the privacy rights of our users, regardless of the format or medium of information in use. This commitment has not changed in the era of the World Wide Web. In fact, it has only strengthened in the years since the Internet was introduced into America's libraries. See for example "Access to Digital Information, Services, and Networks," in which ALA reaffirmed that "Users have both the right of confidentiality and the right of privacy."

Links to selected sample library privacy policies can be found at "Privacy Resources for Librarians, Library Users, and Families." In addition, Part 3, Chapter 4.5, "Guidelines for Developing a Library Privacy Policy," of the *Intellectual Freedom Manual* (2010), discusses the process involved in developing a confidentiality policy.

See : *Chmara, Theresa. Privacy and Confidentiality Issues: a Guide for Libraries and Their Lawyers*. Chicago : American Library Association, 2009

6. What are the privacy rights and responsibilities of staff, volunteers, and trustees?

"Privacy: an Interpretation of the Library Bill of Rights," like the "Library Bill of Rights," itself, addresses the rights of library users. This *Interpretation* also has implications for library staff, educators, volunteers, and trustees. When staff are library users, they are entitled to equal protection of their privacy and confidentiality of their records as library users. They may not, however, be entitled to privacy when acting in their capacity as employees.

Employers have a legitimate interest in ensuring efficiency and productivity. Library management has an obvious further interest in ensuring that employee practices do not adversely impact user service or infringe on user rights, including user rights of privacy and confidentiality. But library employers and educational institutions who use electronic or video surveillance or engage in monitoring of computer, e-mail, or telephone use by employees must carefully evaluate these practices in light of both legal requirements and the profession's ethical commitment to upholding rights of privacy and confidentiality.

*** Legal issues:** Few laws regulate employee monitoring in the private sector, although federal, state, and local government employees benefit from some degree of legal protection. Some state public record and record retention laws may impact the degree to which employee personally identifiable information (PII) is kept confidential. Employee PII not covered by law or regulation must be kept confidential. Further, employees have a right to know what security and information management systems are in place to protect personnel records containing PII, and a right to clear enumeration of the circumstances under which such information may be provided to third parties. Library policy should call for the release of PII to law enforcement requests only when those requests come in the form of a court order from a court of competent jurisdiction. [1]

*** Monitoring:** In many libraries, employees are required to sign Internet and computing use agreements that differ from the policies extended to library users. However, if a library intends to engage in monitoring of staff workstations or work spaces, it should give notice through a written policy providing:

- notice of these practices to employees;
- notice to the public if any staff-user interactions (e.g., virtual reference) are subject to monitoring or recording; and both redaction of PII from and regular purging of all such records;
- notice to employees if their social security numbers are used as unique identifiers in personnel or other records;
- employee access to all PII, including any collected through monitoring, and the right to dispute and delete inaccurate data;
- no monitoring of areas designed for employee health or comfort;
- no collection of data not specifically related to work performance; and;
- restrictions on PII disclosure to third parties without employee consent.

* **Staff use of library resources**: All staff use of library resources or public access workstations that is conducted outside of work hours and/or is not directly job-related should be covered in the same way that any library user's privacy and confidentiality is protected.

For more information on employee privacy rights, and on policy writing to protect those rights, see:

- *Chmara, Theresa. Privacy and Confidentiality Issues: a Guide for Libraries and Their Lawyers*. Chicago : American Library Association, 2009
- American Civil Liberties Union, "Privacy in America: Electronic Monitoring,"
- American Civil Liberties Union, "Through the Keyhole,"
- Electronic Privacy Information Center, "Workplace Privacy Page,"
- Privacy Rights Clearinghouse. "Fact Sheet 7: Workplace Privacy,"

7. What role does education play in protecting patron privacy?

The library should have a continuing training plan to educate adult and student staff, educators, trustees, volunteers, and contract workers about library privacy principles, policies and procedures, and library staff's legal and ethical responsibilities as custodians of personally identifiable information (PII). It is important that all concerned understand that this responsibility includes avoiding any inferences about users based on their library use.

All staff and any others with access to employee PII must understand they are not to look at any stored information without prior authorization to do so, and in accordance with written policies; and that if they accidentally see any such data (such as electronic monitoring logs, e-mail subject lines, file names, etc.) they are bound by confidentiality guidelines.

Library staff should also be informed of their responsibility to cooperate with other organizations that work to protect privacy and challenge intrusions.

Librarians must educate their users through a variety of learning methods that provide the information and tools adults and minors need to protect their privacy and the confidentiality of their own PII. For support in this area, see the

"Privacy and Confidentiality," section of the ALA Office for Intellectual Freedom's Web site.

8. Does privacy include a right to avoid exposure to unwanted images?

Protecting privacy in the library setting ensures open inquiry without fear of having one's interests observed by others. Ensuring user privacy not only benefits the user, but also those who prefer not to see what other users view. When there is a conflict between the right of individuals to view constitutionally protected speech and the sensibilities of unwilling viewers, free expression rights have generally prevailed in the Courts unless unwilling viewers are unable to avert their eyes. Libraries may address the concerns of unwilling viewers in a number of different ways, including the strategic placement of workstations and the use of devices such as privacy screens or recessed monitors.

9. What is a Privacy Audit and whose responsibility is it?

A privacy audit is a technique for assuring that an organization's goals and promises of privacy and confidentiality are supported by its practices, thereby protecting confidential information from abuse and the organization from liability and public relations problems. An audit ensures that information processing procedures meet privacy requirements by examining how information about customers and employees is collected, stored, shared, used and destroyed. Privacy auditing is a process, not a one-time solution, as services, data needs, and technology change. A designated Privacy Officer may lead the audit, but all stakeholders and aspects of privacy need to be represented, from information technology to public relations.

The audit process needs to be capable of dealing with the full extent of the information system. When a library is part of a larger organization such as a university or a K-12 school district that is conducting a privacy audit, specific library issues and needs must be included. The audit process begins by evaluating the organization's existing policies and procedures for legality and consistency with the organization's mission and image. When policies have been reviewed (or established), the data collected can be categorized according to the degree of security necessary. The audit assesses the sensitivity, security risks, and public perceptions of the information the organization collects. The audit examines the necessity for each type of data, how it is collected, and what notice and options are provided to the individuals identified by the information. Mapping how data flows through the organization for access, storage, and disposal can reveal security needs, both electronic and physical. The audit process itself must be managed so that it does not increase risks and its recommendations must be addressed quickly once risks are revealed.

Sources:

Adams, Helen R., Robert F. Bocher, Carol A. Gordon, and Elizabeth Barry-Kessler. *Privacy in the 21st Century: Issues for Public, School, and Academic Libraries*. Westport, Connecticut: Libraries Unlimited, 2005.

Coyle, Karen. 2002. "Privacy and Library Systems Before & After 9/11,"

Enright, Keith P. [2001]. "Privacy Audit Checklist,"

Flaherty, David H. 1998. "How To Do A Privacy And Freedom Of Information Act Site Visit," David H. Flaherty.

II. Protection of Privacy and Library Records

10. Are there special challenges created for library administration by digital patron records?

Any database of personally identifiable information (PII) is a potential target for computer crime and identity theft. Data security must be planned to protect both the library itself and its promise of confidentiality and to ensure the thorough removal of patron records as soon as each ceases to be needed. Library administration should seek ways to permit in-house access to information in all formats without creating a data trail. In general, acquiring the least amount of PII for the shortest length of time reduces the risk of unwanted disclosure. The library should also invest in appropriate technology to protect the security of any PII while it is in the library's custody, and should ensure that aggregate data has been stripped of PII.

In order to assure their obligations of confidentiality, libraries and schools should implement written policies governing data retention and dissemination of electronic records. These policies should affirm the confidentiality of information about library users and their use of all library materials.

See: Chmara, Theresa. Privacy and Confidentiality Issues: a Guide for Libraries and Their Lawyers. Chicago : American Library Association, 2009

11. What else besides library records might compromise user privacy?

It is inevitable that library staff will recognize users. It is also necessary that staff be aware of activity and behavior inside the library to ensure that users' needs are met and for security purposes. This knowledge should not be put to any purpose other than service to library users.

12. How should we work to protect user privacy if our library or institutional policies or services require us to be closely involved with or closely monitoring our library users?

In all libraries, it is the nature of the service rather than the type of the library that should dictate any gathering of personally identifiable information (PII). Some common library practices necessarily involve close communication with — or monitoring of — library users. Services such as bibliographic instruction, reference consultation, teaching and curriculum support in school libraries, readers' advice in public libraries, and preservation of fragile or rare library materials in special collections libraries are just a few instances of services that require library staff to be aware of users' information-access habits. As part of serving the user, it is often necessary for staff to consult with each other. Staff must be careful to conduct such conversations privately and keep strictly to the purpose. But in all types of libraries, any such compromising of user privacy by library staff carries with it an ethical and professional (and often legal) obligation to protect the confidentiality of that PII. Most important, all gathering of PII should be done in the interests of providing, or improving, particular library services.

13. Our library has been using a lot of new technologies in recent years. How can we stay on top of all the privacy concerns?

Every technology since fire can be used for both good and evil. It is the responsibility of librarians to establish policies to prevent any threat to privacy posed by new technologies. It is attention and commitment to fundamental principles of data security that may best ensure that user rights to privacy and confidentiality are not threatened through their use of library services. To help define and assess your local data security practices, consider reviewing these guidelines:

Privacy Rights Clearinghouse, "Fact Sheet 12: Checklist of Responsible Information-Handling Practices,"

Jeff Eisenberg and Connie Lawthers, "Computer and Network Security: Introduction,"

14. Can libraries use social security numbers (SSNs) in patron databases or for other means of uniquely identifying our users?

SSNs are not entirely random numbers: the first three digits indicate in which state the number was issued, and the next two numbers indicate the order in which the SSN was issued in each area. Only the last four numbers are randomly generated. Thus, even the disclosure of an SSN without further action does divulge private information.

Some states restrict the use of social security numbers to circumstances explicitly authorized by law, particularly for the reporting of income for employees. Section 7 of the Federal Privacy Act of 1974 provides that any agency requesting an individual to disclose his or her SSN must "inform that individual whether that disclosure is mandatory or voluntary, by what statutory authority such number is solicited, and what uses will be made of it." The Family Educational Rights and Privacy Act (FERPA) requires publicly-funded schools to obtain written consent for the release of personally identifiable information, which courts have ruled includes SSNs. The widespread use of SSNs by public and private agencies had created a dual threat of fraud victimization and the invasion of privacy, by linking significant amounts of personal and financial information through a single number. In November 2004 the U.S. Government Accountability Office (GAO) in "Social Security Numbers,"noted that ". . . it is clear that the lack of a broad, uniform policy allows for unnecessary exposure of personal Social Security numbers."

Libraries have long used SSNs to trace patrons who have outstanding fines or overdue materials, often through collection agencies. In fact, the current state of Internet technology often allows an individual to be located without the use of an SSN. Libraries that choose to use SSNs in patron databases or to identify users should:

- inform patrons whether providing their SSNs is mandatory or voluntary, and under what statutory authority the SSNs are solicited;
- inform patrons of the purpose for which SSNs will be used;
- use encryption to protect SSNs within patron databases, and;
- investigate other methods of uniquely identifying patrons and tracing those who have outstanding fines or overdue materials.

Sources:

Electronic Privacy Information Center, Social Security Number (SSN) Privacy Page.

Family Educational Rights and Privacy Act (FERPA).

Governmental Accounting Office, "Social Security Numbers: Governments Could Do More to Reduce Display in Public Records and on Identity Cards."

Privacy Act of 1974 and Amendments (as of January 3, 2005).

Privacy Rights Clearinghouse, "My Social Security Number: How Secure Is It?."

Sample library policies:

College of William & Mary, Earl Gregg Swem Library, "Faculty Circulation Services."

American Library Association
http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/qa-privacy

University of California Libraries, http://libraries.universityofcalifornia.edu/privacy/ .

Harvard Libraries, http://lib.harvard.edu/comments/privacy.html.

Shelburne Memorial Library, http://sherlib.wordpress.com/about-us/policies/privacyconfidentiality/.

Seattle Public Library, http://www.spl.org/about-the-library/library-use-policies/confidentiality-of-library-borrower-information.

Mill Valley Public Library, http://www.cityofmillvalley.org/Index.aspx?page=581.

St. Joseph County Public Library, http://sjcpl.lib.in.us/policies/files/PublicServicePolicy2010.pdf.

(See sections 3.0, 3.1.1, 3.1.2 & 3.1.3)

15. How does FERPA impact academic libraries and the privacy of students' library records?

"The Federal Educational Rights and Privacy Act," 20 U.S.C. § 1232g, (FERPA) controls disclosure of a student's educational records and information. It requires educational institutions to adopt policies that permit students to inspect and correct their educational records. It also prohibits disclosure of a student's records without the student's written permission. This applies to the records of any student enrolled at a post-secondary educational institution, even if that student is under the age of 18.

The Family Policy Compliance Office (FPCO), a part of the U.S. Department of Education, is the federal office charged with overseeing and enforcing FERPA. According to FPCO, any record maintained by an educational institution directly related to a student, in any format, that allows the student to be identified from the information contained in it, is considered an "educational record." Analysts within FPCO have issued guidance stating that library circulation records and similar records maintained by a university library are "educational records" under FERPA.

Though FERPA generally requires institutions to protect the privacy of educational records, it contains many exceptions that allow disclosure of a student's educational records without the student's consent or permission. For example, FERPA permits educational institutions to release information contained in a student's records to any school official who has a "legitimate educational interest" in the records; to appropriate public officials in health and safety emergencies; and to courts and law enforcement agencies in response to a judicial order or lawfully issued subpoena. FERPA also permits educational institutions to disclose information about international students to the Department of Homeland Security and the Immigration and Customs Enforcement Bureau. In addition, colleges and universities may disclose records and information to the parents of adult students if the student is a tax dependent or if the student is under 21 and has violated any law or regulation concerning the illegal use of drugs or alcohol.

FERPA thus permits disclosure when state library confidentiality statutes and professional ethics would otherwise prohibit the disclosure of library records. FERPA, however, does not require the institution to disclose records under these circumstances, nor does FERPA require institutions to create or maintain particular records. University and college libraries may therefore draw upon professional ethics and academic freedom principles to craft policies that extend additional privacy protection to users' library records; adopt record retention policies that protect user confidentiality; and, where applicable, incorporate state law protections for library records.

Additional Resources

Family Educational Rights and Privacy Act, 20 U.S.C. 1232g

Code of Federal Regulations, Family educational rights and privacy, 34 C.F.R. Part 99.

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

16. How should we handle additional records kept by the library for the purpose of serving users with special needs?

If libraries create additional records for special purposes, the same responsibility to maintain the confidentiality of those records applies. However, libraries that choose to keep such information on an ongoing basis acquire a correspondingly greater responsibility to maintain the ongoing confidentiality of that information. Policies and procedures should address the collection, retention, and disclosure of records in any format that contain personally identifiable information in compliance with statutory requirements. Libraries should also apply the Fair Information Practice Principles: Notice, Consent, Access, Security and Enforcement. When complying with ALA's "Library Services for People with Disabilities Policy," all attempts should be made to protect the privacy and confidentiality of library users with disabilities. See "Services to Persons with Disabilities: An Interpretation of the Library Bill of Rights."

17. I'd like to let my users pick up their own holds without having to ask for staff assistance. Can I do this while still protecting their confidentiality?

Allowing patrons to pick up their own holds from an open shelf is a popular trend, but one that can violate your library's confidentiality policy and may even violate state laws. Libraries that offer this option should minimize linking a title with a particular user and shield users' names from public view. With these goals in mind, your library can offer this service without abandoning confidentiality. To protect patrons' identities while still allowing them to find their own items, use pseudonyms, codes, numbers or other means of masking identity. Protect the item's identity by wrapping it with a full sheet of paper, using an envelope or reusable bag to hold the item, or some equivalent option. Provide your users with the ability to opt out of the open hold arrangement if they request it.

See "**Resolution to Protect Library User Confidentiality in Self-Service Hold Practices.**"

18. Will smart cards, or ID cards that use biometric enhancements, help protect privacy?

Smart cards are getting a lot of attention for their ability to store personal data for a variety of applications. With the best intentions, government agencies sometimes propose sharing data on people who receive government services. Library policies on confidentiality should state clearly that personally identifiable information collected by the library will not be shared with any other agency or organization unless required by a court order. If agencies are jointly issuing a smart card, library data must be partitioned with no leakage to other agencies.

The more agencies using a shared card, the greater the need for strong identification confirmation. Various biometrics, from photographs to fingerprints to iris scans, are proposed to ensure that identification cards are authentic. This raises correspondingly greater risks that tampering with the encoding of identification will affect every aspect of an individual's life. Biometrics can offer increased convenience, as in the suggestion of children checking out books by thumb print, but the risks must be carefully weighed. Libraries have a responsibility to invite public discussion on the pros and cons of identification technology proposals. The following URLs consider various aspects of new identification card technology:

American Library Association. "Resolution on Privacy and Standardized Driver's Licenses and Personal Identification Cards,"

Barnes, Bill. "The National ID Card: If They Build it, Will it Work?" Slate.

Computer Professionals for Social Responsibility, "National Identification Schemes: Links to Resources."

Electronic Frontier Foundation, "National Identification Systems."

Electronic Privacy Information Center. "National ID and the REAL ID Act."

Ellison, Larry. "Smart Cards: Digital IDs Can Help Prevent Terrorism," Wall Street Journal, Monday, October 8, 2001.

Garfinkel, Simson, "Identity Card Delusions," Technology Review, April 2002.

Glasner, Joanna. "Linking Records Raises Risks," Wired News, April 20, 2001.

Ham, Shane and Robert D. Atkinson. "Frequently Asked Questions about Smart ID Cards," Progressive Policy Institute.

"Smart Card Basics."

19. Should libraries use data encryption to protect privacy?

Some privacy rights advocates encourage increased use of data encryption as a method for enhancing privacy protection. Encrypted data requires others to use a pre-defined electronic "key" to decipher the contents of a message, file, or transaction. While not yet in widespread use by individuals, data encryption is commonly used in online banking and commerce. Libraries should negotiate with vendors to encourage the use of such technology in library systems (e.g., in the document delivery, saved searches, and email features now offered by many OPAC vendors). Whenever possible, libraries should consider making encryption tools available to library users who are engaging in personalized online transactions or communications.

Center for Democracy and Technology, "Resource Library: Encryption"

Electronic Frontier Foundation, "Encryption Archive"

Electronic Privacy Information Center, "Cryptography Policy"

Electronic Privacy Information Center, "EPIC Online Guide to Practical Privacy Tools."

MyCrypto.net, "Encryption and Privacy."

20. My library is considering implementing a Radio Frequency Identification (RFID) system for circulation and stacks maintenance. What are the implications for user privacy of such a system?

Some libraries have already implemented RFID; others are waiting until some of the industry technical standards and privacy implications have been better resolved. ALA has approved "RFID Privacy Principles," that encourage libraries to adopt and enforce privacy policies and discourage inclusion of personal information on RFID tags. When considering, selecting and implementing RFID, libraries should safeguard user privacy by consulting ALA's "RFID in Libraries: Privacy and Confidentiality Guidelines," in order to adopt best practices to protect privacy and confidentiality.

Additional resources are also available:

American Library Association Council, "Resolution on Radio Frequency Identification (RFID) Technology and Privacy Principles."

ALA Library, Fact Sheet 25 - RFID: A Brief Bibliography."

Ayre, Lori Bowen, "RFID,"

Book Industry Study Group. "BISG Policy Statement #002: RFID - Radio Frequency Identification Privacy Principles."

Caldwell-Stone, Deborah, "RFID and Libraries," *Library Technology Reports*, November/December 2010 (46:8)

RFID_LIB–Radio Frequency Identifiers in Library Usage, "About RFID_LIB,"http://listsmart.osl.state.or.us/mailman/listinfo/rfid_lib.

Electronic Privacy Information Center, "Radio Frequency Identification (RFID) Systems."

Beth Givens, "RFID Implementation in Libraries."

David Molnar and David Wagner, "Privacy and Security in Library RFID Issues, Practices, and Architectures."

PRIVACY*notes*, "RFID Position Statement of Consumer Privacy and Civil Liberties Organizations."

21. Can circulation or registration information be used for other library purposes, such as to generate mailing lists for fund-raising by the library or its Friends group?

The Fair Information Practice Principles of "Notice and Openness" and "Choice and Consent" should be reflected in library privacy policies. See "How to Draft a Library Privacy Policy."

Some states impose restrictions on the use of personally identifiable information (PII) for any purposes other than circulation or administration. In other states it is illegal to provide library user PII to any third party except under court order. See "State Privacy Laws Regarding Library Records." In all states, regardless of the status of the law, library policies regarding the collection, use and dissemination of PII should be carefully formulated and administered to ensure that they do not conflict with the ALA Code of Ethics that states "we protect each user's right to privacy and confidentiality." Libraries choosing to use PII for any library-related purpose other than for which the PII was gathered should consider the following standard "opt-in" practices:

- Notice should be provided to all users of any library use of PII.
- Any use of PII beyond circulation or administration should be authorized only on an opt-in basis. At the time of registration, users should be asked to opt-in to additional and specifically enumerated uses of their PII (e.g., for fund-raising appeals). The PII of those who decline to 'opt-in' should not be made available for any additional uses.
- Any time a library decides to extend use of PII in ways not already authorized, it must seek user opt-in. Libraries should presume that all non-responders wish to opt out of the new use.

22. Does the library's responsibility for user privacy and confidentiality extend to licenses and agreements with outside vendors and contractors?

Most libraries conduct business with a variety of vendors in order to provide access to electronic resources, to acquire and run their automated systems, and in some instances, to offer remote storage (e.g. "cloud computing) or to enable access to the Internet. Libraries need to ensure that contracts and licenses reflect their policies and legal obligations concerning user privacy and confidentiality. Whenever a third party has access to personally identifiable information (PII), the agreements need to address appropriate restrictions on the use, aggregation, dissemination, and sale of that information, particularly information about minors. In circumstances in which there is a risk that PII may be disclosed, the library should warn its users.

23. How does the library's responsibility for user privacy and confidentiality relate to the use by library users of third party services in accessing their own circulation records?

Free third-party services are now available that remind library users of due dates and circulation fines via e-mail or RSS feeds. Libraries should advise users about the risks associated with providing library card numbers, passwords, or other library account information to any third party. These risks include changes in the privacy policies of the third-party service without customer notification and disclosure of the user's library circulation records or other personally identifiable information, whether such disclosure is inadvertent or purposeful. Third parties are not bound by library confidentiality statutes or other laws protecting the privacy of user records. For these reasons, neither the library nor the library user can be certain that confidentiality will be adequately protected.

III. Security Concerns

24. Will privacy policies create a situation that will protect illegal acts?

All libraries are advised to have in place patron behavior policies as well as Internet use policies. In both instances it should be clearly stated that engaging in any illegal act will not be permitted. A possible policy statement could be:

Any activity or conduct that is in violation of federal, state, or local laws is strictly prohibited on library premises.

Clear evidence of illegal behavior is best referred to law enforcement who know the processes of investigation that protect the rights of the accused.

25. What about security? Shouldn't priority be given to the legitimate needs of security personnel who are responsible for protecting the physical safety of users and staff? What about the needs of systems personnel to ensure security of computers and networks?

Those responsible for maintaining the security of the library, its users, staff, collections, computing equipment and networks all have a special obligation to recognize when they may be dealing with sensitive or private information. Like other staff whose jobs are not direct library service (principals, teachers and other educators, custodians, guards, etc.), those with access to personally identifiable information (PII) or to users' personal files need to be informed of library ethics and of job expectations that they will not abuse confidentiality.

It is the responsibility of library staff to destroy information in confidential or privacy protected records in order to protect from unauthorized disclosure. Information that should be regularly purged or shredded includes PII on library resource use, material circulation history, and security / surveillance tapes and logs. Libraries that use surveillance cameras should have written policies stating that the cameras are not to be used for anything else to avoid "function creep." If the cameras create any records, the library must recognize its responsibility to protect their confidentiality like any other library record. This is best accomplished by purging the records as soon as their purpose is served.

26. Should staff be instructed to monitor library use to determine inappropriate or illegal behavior by users?

Library patron behavior policies and Internet use policies, should clearly state that illegal activity is prohibited. Staff should be trained carefully to deal with any illegal patron behavior that is apparent to them or has been brought to their attention. General monitoring by staff of the content or use of library materials and resources in any format by patrons is inappropriate in all instances with the exception of observation for the purposes of protecting library property. Patron Behavior and Internet Use policies should clearly state all of the steps to be taken by staff when illegal behavior or activity in violation of the above policies is observed. The steps in these guidelines will vary from library to library and should be

determined locally. Once again, clear evidence of illegal behavior is best referred to law enforcement who know the processes of investigation that protect the rights of the accused.

27. What if law enforcement requests disclosure of library records? What if laws applicable to my library require the disclosure of some or all library records or other personally identifiable information without a court order?

Library policies must not violate applicable federal, state, and local laws. However, In accordance with Article IV of the "Library Bill of Rights," librarians should oppose the adoption of laws that abridge the privacy rights of any library user.

Forty-eight states have statutes that protect the confidentiality of library records. The other two have attorneys' general opinions that support the confidentiality of library records. For your state statute or opinion, see "State Privacy Laws regarding Library Records."

Library policy should require that law enforcement requests for any library record be issued by a court of competent jurisdiction that shows good cause and is in proper form. See ALA's documents, "Suggested Procedures for Implementing Policy on Confidentiality of Library Records,"and "Policy on Confidentiality of Library Records." The library governing authority needs to be aware that privacy, and especially the privacy of children and students may be governed by additional state and federal laws. For example, on April 21, 2000, a new Federal law, the "Children's Online Privacy Protection Act (COPPA)," went into effect. This law, designed to protect children's privacy on the Internet, directly impacts how children access Internet content.

When creating its privacy policies, library and educational institution governing authorities need to be fully aware of any such laws regarding disclosure and the rights of parents, and create policies accordingly. Faculty and school administrators do not have parental authority over students' privacy.

28. My local police department has asked us to voluntarily install "sniffer software" or another kind of spyware on our library computers. What are the implications?

"Sniffer software" are programs that monitor online activity and, once triggered by the use of key words and phrases, can record an online transaction in its entirety. Spyware are programs that record all activity on a computer, such as key-loggers. The records generated by these programs can then be stored for future reference. Even if records are not released unless a law enforcement agency gets a court order, the privacy implications of such a program are significant and serious. First, installing this software in the absence of a court order or patron consent may violate the Electronic Communications Privacy Act (ECPA). Second, the records created by these programs are records of library use, and like all other library user records, are subject to state library confidentiality statutes. Third, a library's mission is to provide access to information, not to serve as a surveillance outpost for law enforcement. Just as we do not keep a history of who checked out library materials (see "Resolution on the Retention of Library Usage Records" 2006*)*, we should not collect and store information from our patrons' online activities.

29. Do library staff have a civic duty to help law enforcement?

If staff observe illegal behavior, this should be reported to law enforcement. A library should have clear, written procedures for responding to criminal behavior, in addition to behavior that violates policy. Neither libraries, their resources, nor their staff should be used in any scheme to elicit and catch criminal behavior.

In the event of a request for information from a federal or local law enforcement agency, librarians should consult with their library administration and/or legal counsel before complying with such requests. Librarians should note that requests made under "The USA PATRIOT Act," must come from the Federal Bureau of Investigation, and are not valid if coming from state agencies. If a librarian is compelled to release information, further breaches of patron confidentiality will be minimized if the librarian personally

retrieves the requested information and supplies it to the law enforcement agency. Otherwise, allowing the law enforcement agency to perform its own retrieval may compromise confidential information that is not subject to the current request.

Library policies protecting patron privacy and confidentiality are grounded in the profession's ethical commitment to providing an atmosphere conducive to free intellectual inquiry. We must always remember that we have a unique and important contribution to make to society through this protection, and that as such we have a duty to make it a priority.

30. Are video or electronic surveillance cameras in libraries a violation of user privacy?

Today's sophisticated high-resolution surveillance equipment is capable of recording patron reading and viewing habits in ways that are as revealing as the written circulation records libraries routinely protect. When a library considers installing surveillance equipment, the administrative necessity of doing so must be weighed against the fact that most of the activity being recorded is innocent and harmless. Any records kept may be subject to Freedom of Information (FOI) requests. Since any such personal information is sensitive and has the potential to be used inappropriately in the wrong hands, gathering surveillance data has serious implications for library management and school administrators.

If the library decides surveillance is necessary, it is essential for the library to develop and enforce strong policies protecting patron privacy and confidentiality appropriate to managing the equipment, including routine destruction of the tapes in the briefest amount of time possible, or as soon as permitted by law.

Such policies should state that the cameras are to be used only for the narrow purpose of enhancing the physical security of the library, its property, staff and patrons.

Policies should also include protocols for posting signs or giving notice about the presence of surveillance cameras; storing of videotapes and other digital images in a secure location; and routine destruction of tapes or images in the briefest amount of time possible, or as soon as permitted by law. If the cameras create any records, the library must recognize its responsibility to protect their confidentiality like any other library record. In addition, some state laws indicate that libraries shall not disclose any information that identifies a person as having used a library or a library service, even if that information is not in the form of a "record." Protecting patron confidentiality is best accomplished by purging the records or images as soon as their purpose is served.

Concerned about increasing school violence, some K-12 schools have installed security cameras in areas where no reasonable expectation of privacy may be expected. This includes computer labs, hallways, cafeterias, and playgrounds. Unfortunately, surveillance equipment has also been installed in some school libraries. It is important that the resulting video is securely handled and that use is based on board approved policy

31. If the library has experienced theft, vandalism, or other suspected criminal activity, may librarians voluntarily supply surveillance camera images to law enforcement?

When library personnel believe that surveillance cameras have recorded evidence of a crime, they should preserve those images and turn them over to the library director or the library's legal counsel, who can then turn over the images to law enforcement in accordance with the law, especially if the images might reveal information about a person's use of specific library resources. Such images may be protected by state library confidentiality laws that prohibit the disclosure of information about a person's use of library materials without a court order.

As a legal matter, libraries may voluntarily disclose surveillance camera images to law enforcement if the images do not reveal any person's use of specific library materials or resources. The decision to disclose surveillance camera images should be made by the library's director in consultation with the library's legal counsel. When state law requires the police to obtain a court order before viewing or copying protected

library records, the library can extend cooperation by identifying relevant records and preserving those records until a court order is served on the library.

IV. Minors' Privacy Rights

32. Are privacy rights of minors the same as those of adults? What information about a minor's use of the library should be kept confidential and what may be released to parents?

The rights of minors vary from state to state. In particular, a minor's right to keep his or her library records private will be governed by a state's library confidentiality statute. Libraries may wish to consult the legal counsel of their governing authorities to ensure that policy and practice are in accord with applicable law. In addition, the legal responsibilities and standing of library staff in regard to minor patrons differ substantially in school and public libraries.

In public libraries, parental responsibility is key to a minor's use of the library. Notifying parents about the library's privacy and confidentiality policies should be a part of the process of issuing library cards to minors. In some public libraries, the privacy rights of minors may differ slightly from those of adults, often in proportion to the age of the minor. The legitimate concerns for the safety of children in a public place can be addressed without unnecessary invasion of minors' privacy while using the library.

Parents are responsible not only for the choices their minor children make concerning the selection of materials and the use of library facilities and resources, but also for communicating with their children about those choices. Librarians should not breach a child's confidentiality by giving out information readily available to the parent from the child directly. Libraries should take great care to limit the extenuating circumstances in which they will release such information.

The rights of minors to privacy regarding their choice of library materials should be respected and protected. More information on the privacy rights of children can be found on the Office for Intellectual Freedom's page "Privacy Resources for Librarians, Library Users, and Families," "Minors and Internet Interactivity: An Interpretation of the Library Bill of Rights," asserts minors' right to interact with, create, and share information on the Internet as extensions of their First Amendment rights. The statement also acknowledges that use of interactive Web 2.0 tools requires the balancing of two competing intellectual freedom priorities — preservation of minors' privacy and the right of free speech.

33. How does the Family Educational Rights and Privacy Act (FERPA) affect minors' library records in K-12 schools?

As with academic libraries, "The Federal Educational Rights and Privacy Act," 20 U.S.C. § 1232g, (FERPA) controls disclosure of a student's educational records and information. It requires educational institutions to adopt policies that permit parents of minor children to inspect and correct their educational records. It also prohibits disclosure of a student's records without the parents' written permission.

The Family Policy Compliance Office (FPCO), a part of the U.S. Department of Education, is the federal office charged with overseeing and enforcing FERPA. According to FPCO, any record maintained by an educational institution directly related to a student, in any format, that allows the student to be identified from the information contained in it, is considered an "educational record." Analysts within FPCO have issued guidance stating that library circulation records and similar records maintained by a school library are "educational records" under FERPA.

Though FERPA generally requires institutions to protect the privacy of educational records, it contains many exceptions that allow disclosure of a student's educational records without a parent's or student's consent or permission. For example, FERPA permits educational institutions to release information contained in a student's records to any school official who has a "legitimate educational interest" in the records; to appropriate public officials in health and safety emergencies; and to courts and law enforcement agencies in response to a judicial order or lawfully issued subpoena. FERPA also permits

educational institutions to disclose information about international students to the Department of Homeland Security and the Immigration and Customs Enforcement Bureau.

FERPA thus permits disclosure when state library confidentiality statutes and professional ethics would otherwise prohibit the disclosure of library records. FERPA, however, does not require the institution to disclose records under these circumstances, nor does FERPA require institutions to create or maintain particular records.

State library confidentiality laws may apply to K-12 libraries as well as public libraries, and may impose additional duties to protect students' library records that go beyond FERPA's requirements/permissions. Therefore, school libraries may therefore draw upon professional ethics and intellectual freedom principles to craft policies that extend additional privacy protection to students' library records; adopt record retention policies that protect students' confidentiality; and, where applicable, incorporate state law protections for students' library records.

34. How can the confidentiality of minors' library records be protected in school libraries?

Each school library should have a privacy policy outlining how students' library records are protected and under what circumstances they may be released and to whom. To do less is to leave the school librarian uncertain about the legal course of action and in a weaker position to respond to requests for release of library records. The privacy policy should reference and incorporate the state library confidentiality law and also incorporate FERPA guidelines.

The policy should also reference American Library Association and American Association of School Librarians policy statements related to protecting minors' privacy rights in libraries. The *Code of Ethics,* states in Article III, "We protect each library users' right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired, or transmitted." The American Association of School Librarians' "Position Statement on the Confidentiality of Library Records" expresses this concept, "The library community recognizes that children and youth have the same rights to privacy as adults." These documents provide an ethical defense for school librarians defending minors' privacy in a school library.

After the privacy policy has been approved by the school's governing body, it should be disseminated to school staff, students, and parents. Minors' privacy and the confidentiality of their records will be better protected when school employees and the community understand the laws involved.

In addition to an official privacy policy, school libraries should also have a records retention policy detailing the types of records maintained, the length of retention, and a schedule for their destruction. Minors' records are best protected when minimal library records are maintained for the shortest period possible.

---

[1] In a June 2010 decision, *City of Ontario v. Quon*, the Supreme Court unanimously upheld the search of a police officer's personal messages on a government-owned pager, saying it did not violate his constitutional rights. The Supreme Court held that the warrantless search was not an unreasonable violation of the officer's 4th Amendment rights because it was motivated by legitimate work-related purposes. In all cases, what constitutes a reasonable search is a question of fact that will be determined by the circumstances of each search.