

Privacy & Confidentiality in Libraries



Illinois Library Association
and the American Library Association



Privacy: An Interpretation of the Library Bill of Rights

Introduction
Rights of Library Users
Responsibilities in Libraries
Conclusion
Notes



Q&A/Privacy: An Interpretation of the Library Bill of Rights

Basic Concepts
Protection of Privacy and Library Records
Security Concerns



Confidentiality and Coping with Law Enforcement Inquiries: Guidelines for Library Staff

Fundamental Principles
General Guidelines
Library Procedures Affect Confidentiality
Recommended Procedures for Law Enforcement Visits

On May 30, 2002, U.S. Attorney General

John Ashcroft and the U.S. Department of Justice issued revised guidelines for the Federal Bureau of Investigation (FBI). As widely reported in the national press, the new guidelines permit FBI agents to monitor public gatherings and conduct surveillance in churches, mosques, and libraries without any evidence that a crime has been committed. The issuance of these new guidelines follows the passage of the U.S.A. Patriot Act, a new law that broadly expands the FBI's ability to access library records.

In a survey of 1,020 public libraries conducted by the University of Illinois' Library Research Center in January and February 2002, 85 libraries reported they had been asked by federal or local law enforcement agents for patron information related to the terrorist attacks on September 11.

Confidentiality
Privacy

In light of these new laws and increased visits to libraries by law enforcement agents, it is important to remember that the underlying Illinois law governing the confidentiality of library users' records has not changed. That law requires any law enforcement agent to present a valid court order showing cause and is in good form before any patron information is disclosed or library records released. This applies to FBI agents, state law enforcement officials, and local police and sheriffs' departments, and includes investigations conducted under the U.S.A. Patriot Act.

Laws governing confidentiality of library records can be found in the *Illinois Compiled Statutes* at 75 ILCS 70/1: "The registration and circulation records of a library are confidential information. Except pursuant to a court order, no person shall publish or make any information contained in such records available to the public."

Privacy: An Interpretation of the Library Bill of Rights

Introduction

Privacy is essential to the exercise of free speech, free thought, and free association. The courts have established a First Amendment right to receive information in a publicly funded library.¹ Further, the courts have upheld the right to privacy based on the Bill of Rights of the U.S. Constitution.² Many states provide guarantees of privacy in their constitutions and statute law.³ Numerous decisions in case law have defined and extended rights to privacy.⁴

In a library (physical or virtual), the right to 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 about users and keeps that information private on their behalf.⁵

Protecting user privacy and confidentiality has long been an integral part of the mission of libraries. The ALA has affirmed a right to privacy since 1939.⁶ Existing ALA policies affirm that confidentiality is crucial to freedom of inquiry.⁷ Rights to privacy and confidentiality also are implicit in the *Library Bill of Rights*⁸ guarantee of free access to library resources for all users.

Rights of Library Users

The *Library Bill of Rights* affirms the ethical imperative to provide unrestricted access to information and to guard against impediments to open inquiry. Article IV states: "Libraries should cooperate with all persons and groups concerned with resisting abridgement of free expression and free access to ideas." When users recognize or fear that their privacy or confidentiality is compromised, true freedom of inquiry no longer exists.

In all areas of librarianship, best practice leaves the user in control of as many choices as possible. These

include decisions about the selection of, access to, and use of information. Lack of privacy and confidentiality has a chilling effect on users' choices. All users have a right to be free from any unreasonable intrusion into or surveillance of their lawful library use.

Users have the right to be informed what policies and procedures govern the amount and retention of personally identifiable information, why that information is necessary for the library, and what the user can do to maintain his or her privacy. Library users expect, and in many places have a legal right, to have their information protected and kept private and confidential by anyone with direct or indirect access to that information. In addition, Article V of the

Library Bill of Rights states: "A person's right to use a library should not be denied or abridged because of origin, age, background, or views." This article precludes the use of profiling as a basis for any breach of privacy rights. Users have the right to use a library without any abridgement of privacy that may result from equating the subject of their inquiry with behavior.⁹

Responsibilities in Libraries

The library profession has a long-standing commitment to an ethic of facilitating, not monitoring, access to information. This commitment

is implemented locally through development, adoption, and adherence to privacy policies that are consistent with applicable federal, state, and local law. Everyone (paid or unpaid) who provides governance, administration, or service in libraries has a responsibility to maintain an environment respectful and protective of the privacy of all users. Users have the responsibility to respect each others' privacy.

For administrative purposes, librarians may establish appropriate time, place, and manner restrictions on the use of library resources.¹⁰ In keeping with this principle, the collection of personally identifiable information should only be a matter of routine or policy when necessary for the fulfillment of the mission of the library. Regardless of the technology

**At
the 2002
American Library
Association Annual
Conference in Atlanta,
Georgia, Privacy: An
Interpretation of the
Library Bill of
Rights was
passed.**

used, everyone who collects or accesses personally identifiable information in any format has a legal and ethical obligation to protect confidentiality.

Conclusion

The American Library Association affirms that rights of privacy are necessary for intellectual freedom and are fundamental to the ethics and practice of librarianship.

- 1 Court opinions establishing a right to receive information in a public library include *Board of Education v. Pico*, 457 U.S. 853 (1982); *Kreimer v. Bureau of Police for the Town of Morristown*, 958 F.2d 1242 (3d Cir. 1992); and *Reno v. American Civil Liberties Union*, 117 S.Ct. 2329, 138 L.Ed.2d 874 (1997).
- 2 See in particular the Fourth Amendment's guarantee of "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," the Fifth Amendment's guarantee against self-incrimination, and the Ninth Amendment's guarantee that "[t]he enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people." This right is explicit in Article Twelve of the Universal Declaration of Human Rights: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." See: <http://www.un.org/Overview/rights.html>. This right has further been explicitly codified as Article Seventeen of the "International Covenant on Civil and Political Rights," a legally binding international human rights agreement ratified by the United States on June 8, 1992. See: http://www.unhchr.ch/html/menu3/b/a_ccpr.htm.
- 3 Eleven state constitutions guarantee a right of privacy or bar unreasonable intrusions into citizens' privacy. Forty-eight states protect the confidentiality of library users' records by law, and the attorneys general in the remaining two states have issued opinions recognizing the privacy of users' library records. See: <http://www.ala.org/alaorg/oif/stateprivacylaws.html>.
- 4 Cases recognizing a right to privacy include: *NAACP v. Alabama*, 357 U.S. 449 (1958); *Griswold v. Connecticut* 381 U.S. 479 (1965); *Katz v. United States*, 389 U.S. 347 (1967); and *Stanley v. Georgia*, 394 U.S. 557 (1969). Congress recognized the right to privacy in the Privacy Act of 1974 and Amendments (5 USC Sec. 552a), which address the potential for government's violation of privacy through its collection of personal information. The Privacy Act's "Congressional Findings and Statement of Purpose" state in part: "the right to privacy is a personal and fundamental right protected by the Constitution of the United States." See: http://caselaw.lp.findlaw.com/scripts/ts_search.pl?title=5&sec=552a.
- 5 The phrase "Personally identifiable information" was established in ALA policy in 1991. See: *Policy Concerning Confidentiality of Personally Identifiable Information about Library Users* (http://www.ala.org/alaorg/oif/pol_user.html). Personally identifiable information can include many types of library records, for instance: information that the library requires an individual to provide in order to be eligible to use library services or borrow materials, information that identifies an individual as having requested or obtained specific materials or materials on a particular subject, and information that is provided by an individual to assist a library staff member to answer a specific question or provide information on a particular subject. Personally identifiable information does not include information that does not identify any individual and that is retained only for the purpose of studying or evaluating the use of a library and its materials and services. Personally identifiable information does include any data that can link choices of taste, interest, or research with a specific individual.
- 6 Article Eleven of the *Code of Ethics for Librarians* (1939) asserted that, "It is the librarian's obligation to treat as confidential any private information obtained through contact with library patrons." See: <http://www.ala.org/alaorg/oif/1939code.html>. Article Three of the current code (1995) states: "We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired, or transmitted." See: <http://www.ala.org/alaorg/oif/ethics.html>.
- 7 See these ALA policies: *Access for Children and Young People to Videotapes and Other Nonprint Formats* (http://www.ala.org/alaorg/oif/acc_chil.html); *Free Access to Libraries for Minors* (http://www.ala.org/alaorg/oif/free_min.html); *Freedom to Read* (<http://www.ala.org/alaorg/oif/freeread.html>); *Libraries: An American Value* (http://www.ala.org/alaorg/oif/lib_val.html); the newly revised *Library Principles for a Networked World* (<http://www.ala.org/oitp/prinintro.html>); *Policy Concerning Confidentiality of Personally Identifiable Information about Library Users* (http://www.ala.org/alaorg/oif/pol_user.html); *Policy on Confidentiality of Library Records* (http://www.ala.org/alaorg/oif/pol_conf.html); *Suggested Procedures for Implementing Policy on the Confidentiality of Library Records* (<http://www.ala.org/alaorg/oif/sugpolcn.html>).
- 8 Adopted June 18, 1948; amended February 2, 1961, and January 23, 1980; inclusion of "age" reaffirmed January 23, 1996, by the ALA Council. See: <http://www.ala.org/work/freedom/lbr.html>.
- 9 Existing ALA policy asserts, in part, that: "The government's interest in library use reflects a dangerous and fallacious equation of what a person reads with what that person believes or how that person is likely to behave. Such a presumption can and does threaten the freedom of access to information." *Policy Concerning Confidentiality of Personally Identifiable Information about Library Users* (http://www.ala.org/alaorg/oif/pol_user.html)
- 10 See: *Guidelines for the Development and Implementation of Policies, Regulations and Procedures Affecting Access to Library Materials, Services and Facilities* (http://www.ala.org/alaorg/oif/pol_reg.html).

Adopted June 19, 2002, by the ALA Council.



The American Library Association has developed this Question and Answer (Q&A) to answer questions raised in comments on Privacy: An Interpretation of the Library Bill of Rights. This Q&A is a work-in-progress; these questions and answers will be further developed and expanded at <http://www.ala.org/alaorg/oif/privacyqanda.html> as more comments are received.

what you bought with your credit card, what you checked out with your library card, or what Web sites you visited. 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. 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. The phrase has been in use in ALA policy since the 1991 adoption of the *Policy Concerning Confidentiality of Personally Identifiable Information about Library Users*, at http://www.ala.org/alaorg/oif/pol_user.html).

Basic Concepts

What is the difference between privacy and confidentiality?

In a library, the right to 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 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 should limit the degree to which personally identifiable information is monitored, collected, disclosed, and distributed.

What is “personally identifiable information?” Why is it such a wordy phrase?

“Personally identifiable information” (PII) seems to have become the generally accepted language because it goes beyond “personal identification,” such as a driver's license. PII connects you to such things as

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. Library buildings, interior design, and functions 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.

What about the rights 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. As such, this new *Interpretation* does have implications for staff, volunteers, and trustees.

When staff are themselves library users, they are entitled to equal protection of the privacy and confidentiality of their records as library users.

If users have rights and librarians have responsibilities, don't users also have responsibilities to protect their own privacy?

Privacy: An Interpretation of the Library Bill of Rights, like the Library Bill of Rights itself, addresses the rights of library users. Text is included in this new *Interpretation* about the right of the user to be informed of library policy and practices that create choices for the user about personal privacy.

Librarians should educate the public, through a variety of methods, about information and tools that can help to preserve privacy or protect the confidentiality of personally identifiable information. In each library transaction in which an individual is asked to divulge personally identifiable information, library staff need to ensure that the individual is making an informed choice. Librarians should clarify any trade-offs between greater convenience and greater privacy. Users also need to understand their own responsibility to respect one another's privacy.

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

Protecting privacy in the library setting ensures open inquiry without fear of having the subject of one's interests observed or examined by others; it is not about protecting people from images or material that may offend them. However, ensuring user privacy not only benefits the user, but also benefits those who prefer not to see whatever the user views. Libraries may address concerns about viewing unwelcome images in a number of different ways, including the strategic placement of workstations and the use of devices, such as privacy screens or recessed monitors. While protecting patrons from exposure to unwanted images is not actually an aspect of privacy, it is nevertheless a by-product of good privacy practices. Again, each individual bears responsibility for respecting and honoring the privacy and right of free inquiry of other library users.

What role does education play in protecting patron privacy?

The library should have an ongoing training plan to educate staff, 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. It is important that all concerned understand that

this responsibility includes avoiding any inferences about users based on their library use.

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 the public through a variety of learning methods that provide the information and tools individuals need to protect their privacy and the confidentiality of their own personally identifiable information.

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 nice 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. Especially when new technology makes issues look different, policies can provide guidance and strength. By establishing strong privacy and confidentiality policies, libraries can protect staff from pressure to violate users' rights.

Protection of Privacy and Library Records

What if our library or institutional policy requires 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. Some common library practices necessarily involve close communication with—or monitoring of—library users. Bibliographic instruction, reference consultation, teaching and curriculum support in school libraries, readers' advisory 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'

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 personally identifiable information. Most important, all gathering of personally identifiable information should be done in the interests of providing, or improving, particular library services.

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.

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 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, 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 personally identifiable information may be disclosed, the library should warn its users.

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 <http://www.ala.org/alaorg/oif/stateprivacylaws.html>.

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* (<http://www.ala.org/alaorg/oif/sugpolcn.html>) and *Policy on Confidentiality of Library Records* (http://www.ala.org/alaorg/oif/pol_conf.html.)

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) (<http://www.ala.org/alaorg/oif/privacy.html>), 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 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.

Chapter 2, part V, of the *Intellectual Freedom Manual* (sixth edition) discusses the process involved in developing a confidentiality policy. See also, "*Developing a Confidentiality Policy*" at <http://www.ala.org/alaorg/oif/frommanual.html>.

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. 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 all instances, best practice is to extend to minor patrons the maximum allowable confidentiality and privacy protections.

My library already has a Web Site Privacy Policy. Where can I go for guidance on what our Web Site Privacy Policy should contain?

This new *Interpretation* 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 Electronic Information, Services, and Networks* (<http://www.ala.org/alaorg/oif/electacc.html>).

Many non-library Web sites now have privacy policies that explain whether personally identifiable information is collected, how it is used if it is collected, and whether they sell or share this information to third parties. Such policies often explain how “cookies” are placed on the hard drive and how they are used to track Web surfing. The privacy policies on governmental Web sites—including governmental library sites—may be covered by applicable local, state, and federal laws. However, regardless of whether such laws are in place or not, libraries of all types—not just those that are publicly funded—need policies outlining the protections in place governing the online and offline privacy and confidentiality rights of library users.

The ALA Intellectual Freedom Committee plans to provide guidance on how to write library Web site policies, outlining steps for effective local implementation of the new Privacy Interpretation. Meanwhile, links to selected sample library privacy policies can be found at *Privacy Resources for Librarians, Library Users, and Families* (<http://www.ala.org/alaorg/oif/privacyresources.html>).

In addition, Chapter 2, part V, of the Intellectual Freedom Manual (sixth edition) discusses the process involved in developing a confidentiality policy. See also, “Developing a Confidentiality Policy” at <http://www.ala.org/alaorg/oif/frommanual.html>.

What about additional records kept by libraries for the purpose of serving patrons 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 (<http://www.ftc.gov/reports/privacy3/fairinfo.htm>).

When complying with ALA's Library Services for People with Disabilities Policy (http://www.ala.org/ascla/access_policy.html), all attempts should be made to protect the privacy and confidentiality of library users with disabilities.

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

Any database of personally identifiable information 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. Library policies should clearly state the purposes for which users' personally identifiable information is needed; these records should be deleted as soon as the original purpose for collection has been satisfied.

In general, acquiring the least amount of personally identifiable information 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 personally identifiable information while it is in the library's custody, and should ensure that aggregate data has been stripped of personally identifiable information.

What about these new smart cards and other new technology—won't they help protect privacy?

Every technology since fire can be used for both good and evil. It is the responsibility of librarians to establish policies to prevent “function creep.” With the best intentions, other 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:

- Barnes, Bill. 2001. *The National ID Card: If They Build it, Will it Work?* Slate.
<http://slate.msn.com/?id=2058321> (accessed July 1, 2002).
- Electronic Privacy Information Center. 2002. *National ID Cards*. http://www.epic.org/privacy/id_cards/ (accessed July 1, 2002).
- Ellison, Larry. 2001. “Smart Cards: Digital IDs Can Help Prevent Terrorism,” *Wall Street Journal*, Monday, 8 October 2001,
<http://opinionjournal.com/extra/?id=95001336> (accessed July 1, 2002).
- Garfinkel, Simson. 2002. “Identity Card Delusions,” *Technology Review*, April 2002,
<http://www.technologyreview.com/articles/garfinkel0402.asp> (accessed July 1, 2002).
- Glasner, Joanna. 2001. *Linking Records Raises Risks*. Lycos Worldwide,
<http://www.wired.com/news/business/0,1367,43061,00.html> (accessed July 1, 2002).

- Ham, Shane and Robert D. Atkinson. 2002. *Frequently Asked Questions about Smart ID Cards*. Progressive Policy Institute, http://www.ppi-online.org/ppi_ci.cfm?knlgAreaID=140&subse-cid=290&contentid=250075 (accessed July 1, 2002).
- Computer Professionals for Social Responsibility. 2002. *National Identification Schemes: Links to Resources*. <http://www.cpsr.org/program/natlID/natlIDlinks.html> (accessed July 1, 2002).
- Wiggins, Dion. 2002. *Big Brother - Real-Time Behavioral Monitoring*. Gartner, Inc.,
<http://www.gartner.com/DisplayDocument?id=351518> (accessed July 1, 2002).
- Wylie, Margie. 2001. *Database Flaws Could Hamper Any National ID System, Experts Warn*. Newhouse News Service,
<http://www.newhouse.com/archive/story1a122001.html> (accessed July 1, 2002).

Security Concerns

What about library staff's 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 U.S.A. Patriot Act (<http://www.ala.org/alaorg/oif/usapatriotact.html>) must come from the Federal Bureau of Investigation (FBI) 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.

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 video 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.

If the library decides video 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.

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? And 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 (custodians, guards, etc), those with access to personally identifiable information 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 prevent unauthorized disclosure. Information that should be regularly purged or shredded includes personally identifiable information 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. If the cameras create any video 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.

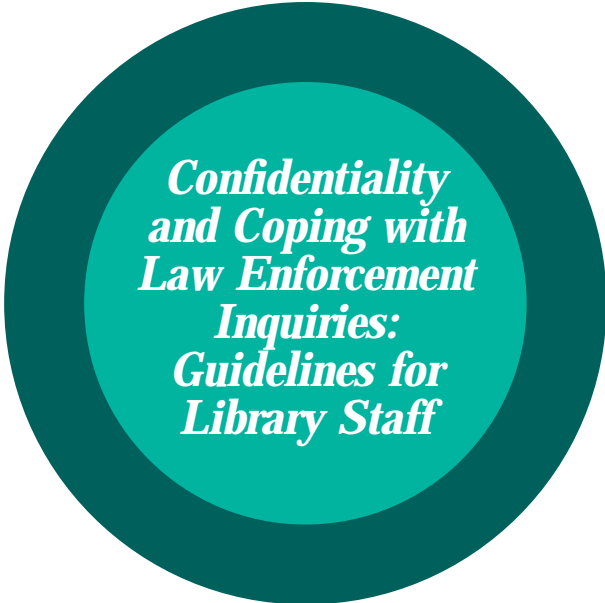
Won't privacy policies create a situation that will protect illegal acts?

All libraries are advised to have 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.

Should staff be instructed to monitor library use by patrons to determine inappropriate or illegal behavior?

Library Patron Behavior policies and Internet Use policies should clearly state that illegal activity is prohibited. Staff should be carefully trained to deal with any illegal patron behavior that is apparent to them or has been brought to their attention. General monitoring by staff of patron content or use of library materials and resources in any format 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.



Confidentiality and Coping with Law Enforcement Inquiries: Guidelines for Library Staff

Increased visits to libraries by law enforcement agents, including FBI agents and officers of state, county, and municipal police departments, are raising considerable concern among the public and the library community. These visits are not only a result of the increased surveillance and investigation prompted by the events of September 11, 2001, and the subsequent passage of the U.S.A. Patriot Act, but also a result of law enforcement officers investigating computer crimes, including e-mail threats and possible violations of the laws addressing online obscenity and child pornography.

These guidelines, developed to assist libraries and library staff in dealing with law enforcement inquiries, rely upon ALA's *Policy on the Confidentiality of Library Records; Policy Concerning Confidentiality of Personally Identifiable Information about Library Users*; and the *Code of Ethics*.

Fundamental Principles

Librarians' professional ethics require that personally identifiable information about library users be kept confidential. This principle is reflected in Article III of the *Code of Ethics*, which states that "[librarians] protect each library user's right to privacy and confidentiality with respect to information sought or received, and resources consulted, borrowed, acquired, or transmitted."

Currently, 48 states and the District of Columbia have laws protecting the confidentiality of library records, and the attorneys general of the remaining two states, Hawaii and Kentucky, have ruled that library records are confidential and may not be disclosed under the laws governing open records. Confidential library

records should not be released or made available in any format to a federal agent, law enforcement officer, or other person unless a court order in proper form has been entered by a court of competent jurisdiction after a showing of good cause by the law enforcement agency or person seeking the records.

General Guidelines

Confidentiality of library records is a basic principle of librarianship. As a matter of policy or procedure, the library administrator should ensure that:

- The library staff and governing board are familiar with the ALA *Policy on the Confidentiality of Library Records, Policy Concerning Confidentiality of Personally Identifiable Information about Library Users*, and other ALA documents on users' privacy and confidentiality.
- The library staff and governing board are familiar with their state's library confidentiality statute or attorney general's opinion.
- The library adopts a policy on users' privacy and confidentiality, which includes procedures for the staff and board to follow if the library is served with a court order for records or if law enforcement agents conduct inquiries in the library.
- The library staff is familiar with the library's policy on confidentiality and its procedures for handling court orders and law enforcement inquiries.

Library Procedures Affect Confidentiality

Law enforcement visits aside, be aware that library operating procedures have an impact on confidentiality. The following recommendations are suggestions to bring library procedures into compliance with most state confidentiality statutes, ALA policies on confidentiality and its Code of Ethics:

- Avoid creating unnecessary records. Only record a user's personally identifiable information when necessary for the efficient operation of the library.
- Avoid retaining records that are not needed for efficient operation of the library. Check with your local governing body to learn if there are laws or policies addressing record retention and in conformity with these laws or policies, develop policies on the length of time necessary to retain a record. Assure that all kinds and types of records are covered by the policy, including data-related logs, digital records, and system backups.

- Be aware of library practices and procedures that place information on public view; e.g., the use of postcards for overdue notices or requested materials, staff terminals placed so that the screens can be read by the public, sign-in sheets to use computers or other devices, and the provision of titles of reserve requests or interlibrary loans provided over the telephone to users' family members or answering machines.

Recommended Procedures for Law Enforcement Visits

Before any visit:

- Designate the person or persons who will be responsible for handling law enforcement requests. In most circumstances, it should be the library director, and, if available, the library's legal counsel.
- Train all library staff, including volunteers, on the library's procedure for handling law enforcement requests. They should understand that it is lawful to refer the agent or officer to an administrator in charge of the library, and that they do not need to respond immediately to any request.
- Review the library's confidentiality policy and state confidentiality law with library counsel.
- A court order may require the removal of a computer workstation or other computer storage device from the library. Have plans in place to address service interruptions and any necessary backups for equipment and software.

During the visit:

- Staff should immediately ask for identification if they are approached by an agent or officer, and then immediately refer the agent or officer to the library director or other designated officer of the institution.
- The director or officer should meet with the agent with library counsel or another colleague in attendance.
- If the agent or officer does not have a court order compelling the production of records, the director or officer should explain the library's confidentiality policy and the state's confidentiality law, and inform the agent or officer that users' records are not available except when a proper court order in good form has been presented to the library.

- Without a court order, neither the FBI nor local law enforcement has authority to compel cooperation with an investigation or require answers to questions, other than the name and address of the person speaking to the agent or officer. If the agent or officer persists, or makes an appeal to patriotism, the director or officer should explain that, as good citizens, the library staff will not respond to informal requests for confidential information, in conformity with professional ethics, First Amendment freedoms, and state law.

- If the agent or officer presents a court order, the library director or officer should immediately refer the court order to the library's legal counsel for review.

If the court order is in the form of a subpoena:

- Counsel should examine the subpoena for any legal defect, including the manner in which it was served on the library, the breadth of its request, its form, or an insufficient showing of good cause made to a court. If a defect exists, counsel will advise on the best method to resist the subpoena.¹
- Through legal counsel, insist that any defect be cured before records are released and that the subpoena is strictly limited to require release of specifically identified records or documents.
- Require that the agent, officer, or party requesting the information submit a new subpoena in good form and without defects.
- Review the information that may be produced in response to the subpoena before releasing the information. Follow the subpoena strictly and do not provide any information that is not specifically requested in it.
- If disclosure is required, ask the court to enter a protective order (drafted by the library's counsel) keeping the information confidential and limiting its use to the particular case. Ask that access be restricted to those persons working directly on the case.

If the court order is in the form of a search warrant:

- A search warrant is executable immediately, unlike a subpoena. The agent or officer may begin a search of library records as soon as the library director or officer is served with the court's order.

- Ask to have library counsel present before the search begins in order to allow library counsel an opportunity to examine the search warrant and to assure that the search conforms to the terms of the search warrant.
- Cooperate with the search to ensure that only the records identified in the warrant are produced and that no other users' records are viewed or scanned.

If the court order is a search warrant issued under the Foreign Intelligence Surveillance Act (FISA/U.S.A. Patriot Act amendment):

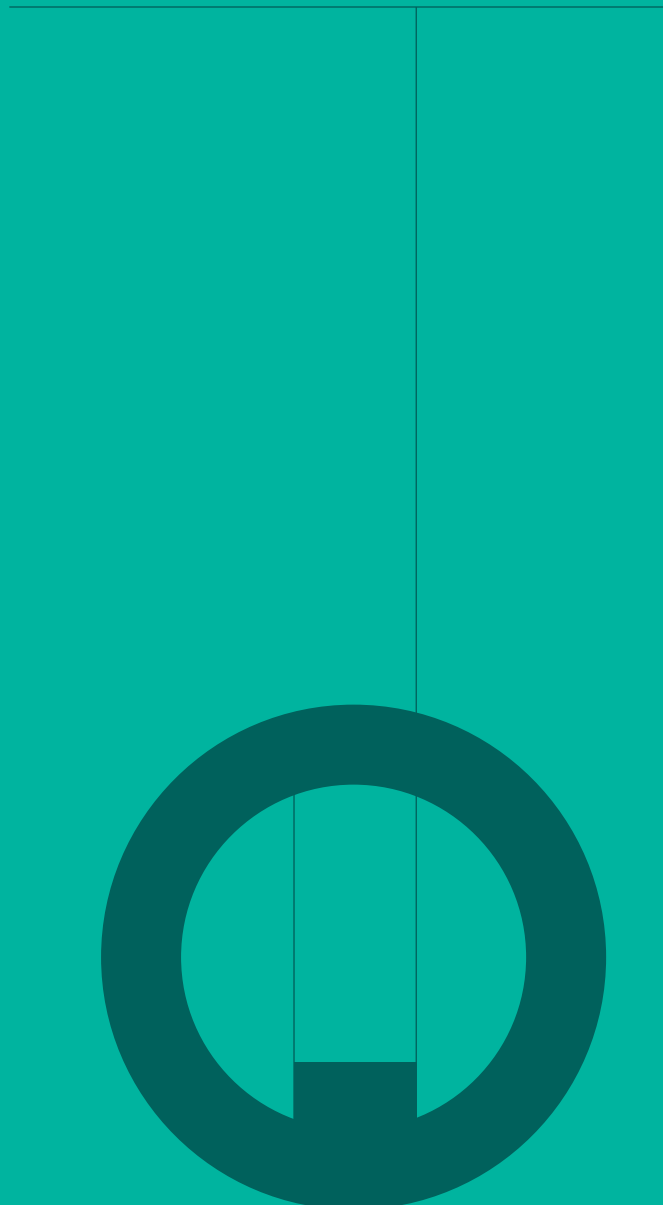
- The recommendations for a regular search warrant still apply. However, a search warrant issued by a FISA court also contains a "gag order." That means that no person or institution served with the warrant can disclose that the warrant has been served or that records have been produced pursuant to the warrant.
- The library and its staff must comply with this order. No information can be disclosed to any other party, including the patron whose records are the subject of the search warrant.
- The gag order does not change a library's right to legal representation during the search. The library can still seek legal advice concerning the warrant and request that the library's legal counsel be present during the actual search and execution of the warrant.
- If the library does not have legal counsel and wishes legal advice, the library can obtain assistance from Jenner & Block, the Freedom to Read Foundation's legal counsel. Simply call the Office for Intellectual Freedom (1-800-545-2433, ext. 4223) and inform the staff that you need legal advice. OIF staff will assure that an attorney from Jenner & Block returns your call. You do not have to and should not inform OIF staff of the existence of the warrant.

After the visit:

- Review the court order with library counsel to ensure that the library complies with any remaining requirements, including restrictions on sharing information with others.
- Review library policies and staff response and make any necessary revisions in light of experience.

- Be prepared to communicate with the news media. Develop a public information statement detailing the principles upholding library confidentiality that includes an explanation of the chilling effect on First Amendment rights caused by public access to users' personally identifiable information.
- If possible, notify the ALA about your experience by calling the Office for Intellectual Freedom at 800-545-2433, extension 4223.

- 1 Usually, the library can file a motion to quash the subpoena or a motion for a protective order. Normally, a hearing is held where the court will decide if good cause exists for the subpoena or if it is defective, and then decide whether the library must comply with the subpoena. Consult with counsel on all issues, including the payment of costs if the library is the unsuccessful party.



Robert P. Doyle
Executive Director

Illinois Library Association
33 West Grand Avenue, Suite 301
Chicago, IL 60610-4306

phone: 312-644-1896
fax: 312-644-1899
e-mail: ila@ila.org
www.ila.org

July 2002

-
1. Library records are protected in Illinois by statute.
 2. Newly passed federal legislation—the U.S.A. Patriot Act—expands the scope of inquiries by law enforcement into library records, but patrons’ rights to privacy and confidentiality remain unchanged.
 3. In a library, the right to privacy is the right to open inquiry without having the subject of one’s interest examined or scrutinized by others.
 4. Confidentiality exists when a library is in possession of personally identifiable information about users and keeps that information private on their behalf.
 5. Libraries should limit collection of personally identifiable information to the minimum necessary to provide service.
 6. All libraries are advised to have patron behavior and Internet policies stating clearly that any illegal act will not be permitted; if any illegal behavior is observed, staff should report it to law enforcement.
 7. In the event of a request for information about a patron’s records from a federal, state, or local enforcement agency, librarians should consult with their administration and/or legal counsel before complying.
-

Single copies of *Privacy and Confidentiality in Libraries* are available free.
Multiple copies are available in packets of 25 copies for \$12 plus \$2 shipping via library rate.