Privacy Tool Kit

American Library Association

Office for Intellectual Freedom &

Intellectual Freedom Committee

Privacy is essential to the exercise of free speech, free thought, and free association. Lack of privacy and confidentiality chills users' choices, thereby suppressing access to ideas. The possibility of surveillance, whether direct or through access to records of speech, research and exploration, undermines a democratic society.—*Privacy: An Interpretation of the Library Bill of Rights*

Table of Contents

Available online at www.ala.org/advocacy/privacyconfidentiality/toolkitsprivacy/privacy
Permission is granted for libraries to reprint the Privacy Toolkit.

Introduction

The first Privacy Tool Kit was created by ALA in 2005, and many changes have occurred in the intervening years, most notably the explosion of technology and social media use which has impacted the privacy of users in all types of libraries. Technology is a blessing and a curse. It has provided opportunities like user-created content and interactivity. Library users are now not only consuming information, they are creating it. Many barriers to access have fallen, but others, like filters, have arisen. Governments and corporations can now capture user information and use it for various purposes—often without the user's knowledge. The danger of invasion of personal privacy is a very real concern and often challenges existing library state privacy and confidentiality laws. In some cases, the existing Library Bill of Rights and Interpretations can be applied, but in others, they need to be amplified. In too many cases, busy librarians are not making the connections between new technology and the threats to users in the form of invasion of privacy. This threat to privacy stifles intellectual freedom and the freedom to read. Despite technology, the desire to protect library users' privacy is strong. The current issues and threats, potential solutions, and resources can be found in the Privacy Tool Kit.

Privacy and Confidentiality: Library Core Values

Privacy is essential to the exercise of free speech, free thought, and free association. Lack of privacy and confidentiality chills people's choices, thereby suppressing access to ideas. The possibility of surveillance, whether direct or through access to records of speech, research and exploration, undermines a democratic society. In libraries, the right to privacy is the right to open inquiry without having the subject of one's interest examined or scrutinized by others.

Confidentiality of library records is a core value of librarianship. Confidentiality exists when a library is in possession of personally identifiable information (PII) about users and keeps that information private on their behalf. This includes such library-created records as closed-stack call slips, computer sign-up sheets, registration for equipment or facilities, circulation records, Web sites visited, reserve notices, or research notes. One cannot exercise the right to read in any format if the possible consequences include damage to one's reputation, ostracism from the community or workplace, or criminal penalties. Consider patrons looking for a new job or information about rock climbing or skydiving; this is information that the current employer or insurance company would like to have. Choice requires both a varied selection and the assurance that one's choice is not monitored.

For libraries to flourish as centers for uninhibited access to information, librarians must stand behind their users' right to privacy and freedom of inquiry. Just as people who borrow murder mysteries are unlikely to be murderers, so those seeking information about terrorism are unlikely to be terrorists. Assuming a sinister motive based on library users' reading choices makes no sense and leads to fishing expeditions that both waste precious law enforcement resources and have the potential to chill Americans' inquiry into current events and public affairs.

The Code of Ethics of the American Library Association and its Library Bill of Rights acknowledge the paramount importance of library patron privacy:

ALA Code of Ethics (first passed, 1939; amended, 1981, 1995, and 2008). "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."

Privacy: an Interpretation of the Library Bill of Rights (2002). "The American Library Association affirms that rights of privacy are necessary for intellectual freedom and are fundamental to the ethics and practice of librarianship."

Selected Links:

- American Library Association, Privacy Policies and Statements
- History of the Code of Ethics, 1930 Suggested Code of Ethics from American Library Association Bulletin
- American Library Association, Questions and Answers on Privacy and Confidentiality, 23 January 2012.

Through the Library Bill of Rights and the ALA Code of Ethics, librarians fight to protect patron privacy and preserve our democratic society by promoting a diversity of viewpoints and ideas to support an informed, literate, and educated public. This Privacy Took Kit will provide you with practical steps you can take to protect patron privacy and confidentiality.

Privacy Policies and the Law

Library privacy and confidentiality policies must be in compliance with applicable federal, state, and local laws. The courts have upheld the right to privacy based on the Bill of Rights of the U.S. Constitution. Many states provide guarantees of privacy in their constitutions and statute law. Numerous decisions in case law have defined and extended rights to privacy.

The Fourth Amendment and a Supreme Court decision are crucial in current discussions of privacy in the library and the extent to which library users have an "expectation of privacy." This is important because in order to determine the extent of Fourth Amendment protection of personally identifiable information, the courts rely heavily on the U.S. Supreme Court decision in *Katz v. United States*, 389 U.S. 347 (1967), which held that the Fourth amendment "protects people, not places" and what a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."

In the Katz decision the Court also reiterated that "the person's general right to privacy – his right to be let alone by other people – is like the protection of his property and of his very life, left largely to the law of the individual states." In all 50 states and the District of Columbia, state constitutions, attorney general opinions, or state library confidentiality statutes provide that protection.

It is, therefore, critical that librarians regularly scrutinize all their library's policies and practices to ensure that, to the greatest extent possible, they support an environment in which the library user's privacy is respected and preserved. It is also important that libraries make every effort to communicate to library users and the communities they serve the importance of the confidentiality of library use in order to protect their intellectual freedom. If we fail to do this the courts may come to the conclusion that individuals no longer expect that the nature of their library use will be protected and, therefore, that privacy will no longer be constitutionally protected.

Selected Links:

- First, Fourth, Fifth, Ninth, Tenth, and Fourteenth Amendments to the Constitution of the United States
- Article Twelve of the Universal Declaration of Human Rights
- Your Privacy Protection Under the Law
- History of the Privacy Act of 1974
- Privacy and the Courts
- State Privacy Laws Regarding Library Records

Standard Privacy Principles

In addition to ALA policies, there are many very good frameworks for establishing privacy policies. The privacy policy guidelines outlined here are based in part on what are known as the five "Fair Information Practice Principles." These five principles outline the rights of Notice, Choice, Access, Security, and Enforcement. Another widely accepted European legal framework establishing rights of data privacy and confidentiality calls for ensuring Collection limitation, Data quality, Purpose specification, Use limitation, Security safeguards, Openness, Individual participation, and Accountability. These frameworks provide the basis for recommendations from other consumer and privacy advocacy groups, whose checklists are well worth reviewing.

Selected Links:

- United States Federal Trade Commission. "Fair Information Practice Principles." (1973)
- Organization for Economic Cooperation and Development (OECD), Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Sept. 1980)
- International Federation of Library Associations (IFLA), "The Glasgow Declaration on Libraries, Information Services and Intellectual Freedom," (The Hague, Netherlands: IFLA, August 20, 2002)
- International Federation of Library Associations (IFLA), "The IFLA Internet Manifesto" (The Hague, Netherlands: IFLA, August 23, 2002)
- Canadian Library Association. 2012. "CLA Position Statement on Access to Information and Communication Technology" (May 29, 2012)
- Privacy Rights Clearinghouse, Fact Sheet 12. A Checklist of Responsible Information-Handling Practices (Revised July 2013)
- Computer Professionals for Social Responsibility, Electronic Privacy Principles

PII: Personally Identifiable Information

One of the key concepts to understand when developing policies and procedures is that defined as: "Personally identifiable information" (PII). ALA Council approved the "Policy Concerning Confidentiality of Personally Identifiable Information about Library Users" in 1991 and amended it in 2004. PII connects individuals to what they've bought with their credit cards, what they've checked out with their library cards, what Web sites they've visited, where they've picked up cookies and what avatars they've registered. PII can easily be linked to every hash tag, like, tweet, post and social media interaction a user makes. More than simple identification, PII can create a picture of 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 an individual's character, decide if they were a security risk, or embarrass them for opposing a particular position. 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.

Selected Links:

- American Library Association, Policy Concerning Confidentiality of Personally Identifiable Information about Library Users (Amended June 30, 2004).
- Privacy Rights Clearinghouse, Privacy Survival Guide (Revised June 2013).

Developing or Revising a Library Privacy Policy

All types of libraries are urged to draft, adopt and/or revise privacy and confidentiality policies. This document offers guidance for public, academic, research, school, and special libraries, as well as library systems. Special considerations are raised for school and academic libraries and for public library services to minors because each are affected by laws and practices unique to those particular contexts. Other considerations may also apply. When drafting a policy, library administrators should check with their parent institutions to ensure compliance with those institutions' norms and policies. Some elements of this guidance may not pertain to all libraries.

In addition, policy drafts should be reviewed against existing local policies, state and local laws, and ALA recommendations and guidelines. Policy drafting teams and trainers may find it helpful to ask themselves and their staff questions from the checklists in the Privacy Audit section and to consider how and whether policies and procedures under consideration provide appropriate guidance.

With technology changes, increased incidence of identity theft, new laws, and increased law enforcement surveillance, librarians must act now to develop and/or revise their privacy policies and procedures to ensure that confidential information in all formats is protected from abuse. They must also protect their organizations from liability and public relations problems. When developing and revising policies, librarians need to ensure that they:

- limit the degree to which the library and third party service providers monitor, collect, disclose, and distribute personally identifiable information;
- avoid creating unnecessary records including non-text records such as camera recordings;
- avoid retaining records that are not needed for efficient library operation, including data-related logs, digital records, vendor-collected data, and system backups;
- avoid library practices and procedures that place personally identifiable information in public view; and
- require that patron records remain on a local server and not be exported to the cloud or a third-party server.

A privacy policy communicates the library's commitment to protecting users' personally identifiable information. A well-defined privacy policy tells library users how their information is utilized and explains the circumstances under which personally identifiable information might be disclosed. When preparing a privacy policy, librarians need to consult an attorney to ensure that the library's statement harmonizes with state and federal laws governing the collection and sharing of personally identifiable information and confidential records.

Libraries need to post privacy policies publicly. Privacy: An Interpretation of the Library Bill of Rights states that, "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."

Sources:

- Carolyn Caywood, "Questions and Answers about Privacy in Libraries," presented at the Virginia Library Association 2002 Conference, October 17, 2002.
- "Confidentiality Inventory," in Confidentiality in Libraries: An Intellectual Freedom Modular Education Program Trainer's Manual (Chicago: ALA, 1993), p. 30.
- Barbara Jones, "Intellectual Freedom Policies for Privacy," Libraries, Access, and Intellectual Freedom: Developing Policies for Public and Academic Libraries (Chicago: ALA, 1999), p. 147-168.
- Confidentiality in Libraries: An Intellectual Freedom Modular Education Program Trainer's Manual (Chicago: ALA, 1993).

A Privacy Audit

A privacy audit of current policies and practices can be an excellent first step in developing a library policy. It will provide insights into strengths and weakness embodied in the existing library's culture. If not conducted early in the development or revision of a privacy policy, a privacy audit should be conducted before the conclusion of the process and should be repeated regularly thereafter.

Definition and Purpose

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 the library collects, stores, shares, uses and destroys information about library users and employees. Privacy auditing is not a one-time solution, but rather a process that adapts to changes in services, data needs, and technology. 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 auditing process should be comprehensive enough to address all relevant nuances of the information system. When a library is part of a larger organization conducting a privacy audit, the audit must include specific library issues and needs.

The auditing 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 of each type of data, how it is collected, and what notice and options are provided to individuals the information identifies. Mapping how data flows through the organization for access, storage, and disposal can reveal security needs, both electronic and physical. The management of the auditing process must avoid increasing privacy risks and its recommendations regarding revealed risks must be addressed quickly.

A privacy audit provides a library opportunity to examine:

- how privacy matters are handled at all levels;
- the flow and storage of data;
- the role data plays within the organization;
- staff training about privacy matters; and
- existing and needed privacy policies.

Selected Sources:

- California Digital Library, SOPAG Privacy Audit and Guidelines
- Karen Coyle, Make Sure You Are Privacy Literate," Library Journal, v. 127, #16, October 1, 2002.
- Karen Coyle, Privacy and Library Systems Before & After 9/11, 2002.
- Keith P. Enright, Privacy Audit Checklist, 2001.
- David H. Flaherty, How To Do A Privacy And Freedom Of Information Act Site Visit, 2001.
- Pamela Jerskey, Ivy Dodge, and Sanford Sherizen, The Privacy Audit: a Primer, 1998.
- Royal, K. "What Makes a Good Privacy Officer?" (2014) Web. 24 Feb. 2014.
- Texas Department of Information Resources, Privacy Issues Involved in Electronic Government, 2000.

What to Audit for Personally Identifiable Information

(Based on: Karen Coyle, Make Sure You Are Privacy Literate," Library Journal, v. 127, #16: reprinted with permission)

- Patron records
- Circulation transaction logs
- Overdue and billing records

- Document delivery and ILL transactions
- Records of access to electronic reserves
- Records that support personalized services
- Search histories saved beyond a session
- Saved searches and sets
- SDI profiles
- Files/logs of previous electronic reference queries and answers
- System logs
- OPAC search logs
- Library web server logs, including proxy servers
- Mail message files
- Mail server logs
- Public workstations
- Browser caches, including history files
- Cookies and certificates
- Browser bookmarks
- Paper sign-up sheets
- Licensed services
- Shared computer systems and servers
- Back up files stored locally and off site
- Remote Web sites, including content providers, outsourced Web hosting, proxy servers, etc.
- Personalization profiles and other service offers for personal information
- Usage statistics.
- Signed Internet/e-mail acceptable use agreements
- User-created lists
- Reviews
- Tags on catalog
- E-book downloads
- Program registrations

Questions to Ask:

Library Privacy Policy: Do you or have you…

- already created and publicized a local privacy policy using the recommendations and resources made available through the Privacy Tool Kit?
- implemented a privacy auditing process to assure that an organization's practices

support its goals and promises of privacy and confidentiality, thereby protecting confidential information from abuse and the organization from liability and public relations problems?

- Limit the degree to which personally identifiable information is monitored, collected, disclosed, and distributed?
- avoid retaining records that are not needed for efficient operation of the library?
- know how long you need to know specific information and do you delete it when no longer needed?
- list information to be protected: reference requests, information services, circulation and registration records, server and client computer logs?
- include language to deal with unforeseen circumstances, like "including, but not limited to . . ."?
- require that patrons be notified whenever the library collects their PII and be told how to correct inaccurate information?
- state who may or may not have access to patron information?
- outline the specific conditions under which access may be granted, i.e., with a court order after good cause has been demonstrated?
- list the procedures for adopting the policy?
- have provisions for notifying the public of the policy and of changes in the policy?
- enumerate exemptions, exceptions, or special conditions? Do you address needs unique to your library environment?
- have provisions for coordination with the other libraries in your system if your library is part of a cooperative, automated library system?
- have procedures outlined for responding to court orders of various types?
- assure that all kinds and types of records are covered by the policy, including data-related logs, digital records, vendor-collected data, and system backups?
- know how you protect what you collect?
- work to inform/influence government acts that impact confidentiality?
- avoid library practices and procedures that place information on public view (e.g., using postcards for overdue notices or requested materials; using patron names to identify self-pickup holds; positioning staff terminals so that the public can read the screens; using sign-in sheets for computer or other device access; and stating reserve request or interlibrary loan titles over the telephone and to voicemail possibly disclosing that information to patrons' family members)?
- include all aspects of services including protection of electronic data and dissemination of electronic records?
- ensure that contracts and licenses reflect library policies and legal obligations

concerning user privacy and confidentiality; make sure the agreements address appropriate restrictions on the use, aggregation, dissemination, and sale of personally identifiable information, particularly information about minors?

- provide privacy where you should?
- ensure safety without being intrusive?
- make clear the role of confidentiality in protecting intellectual freedom?
- know where users need privacy to protect their intellectual freedom as well as where privacy might endanger safety?
- mention or acknowledge the Library Bill of Rights, Statement on Professional Ethics, ALA Policy on the Confidentiality of Library Records, and state & local laws (where applicable)? Does your policy conform to these supporting documents?

Protecting Minors' Privacy: Do you or have you…

- extend to minors the maximum allowable confidentiality and privacy protections?
- notify parents about the library's privacy and confidentiality policies when issuing library cards to minors?
- educate children, parents, students, teachers, and school officials about the Children's Online Privacy Protection Act (COPPA) and the Family Educational Rights and Privacy Act (FERPA)? COPPA requires commercial Web sites and online services to obtain parental permission before collecting information from children under 13. FERPA requires educational institutions to protect students' privacy with regard to educational records.

Educating about Privacy: Do you or have you…

- educate on a continuous basis everyone associated with the library about library privacy principles, policies and procedures, and library staff's legal and ethical responsibilities as custodians of personally identifiable information? Those associated with the library include library trustees, users, and employees (e.g., staff, administrators, volunteers, and contract workers); those associated with school and academic libraries include school board trustees, educational administrators, students, and parents.
- inform library staff about their responsibility to cooperate with other organizations that work to protect privacy and challenge intrusions?
- engage the community in considering the public policy aspects of privacy through use of Choose Privacy Week materials at (http://chooseprivacyweek.org/)
- 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?
- inform the public about library resources on privacy issues?

- give users choices?
- explain to the public the difference between privacy and confidentiality in a library setting?

Sections or Issues to Include in a Privacy Policy

Notice & Openness

Policies should notify users of their rights to privacy and confidentiality and of the policies of the library that govern these issues. Such notice should dictate the types of information gathered and the purposes for and limitations on its use. It is critical that library privacy policies be made widely available to users through multiple means. Safeguarding personal privacy requires that individuals know what personally identifiable information (PII) is gathered about them, where and how and for how long it is stored, who has access to it and under what conditions, and how it is used.

Examples of User Notice Statements from Sample Library Privacy Policies:

- Mill Valley Public Library Privacy Statement
- Queens Borough Public Library
- Rutgers University Library

Choice & Consent

Choice means giving users options as to how any personal information collected from them may be used. Provision of many library services requires the collection and retention of personally identifiable information. Whether this is required (e.g. in order to circulate library material), automatic (e.g. as in some Web-based library services), or voluntary (e.g. when engaging in e-mail-based reference), the library should retain this information only as long as is necessary to fulfill the function for which it was initially acquired. Two commonly used schemes for choice/consent are "opt-in" and “opt out”. With opt-in, by default PII is not included and affirmative steps are required for inclusion. With opt-out, by default PII is included and affirmative steps are required for exclusion.

Examples of Choice and Consent Statements from Sample Library Privacy Policies:

- Chemung County Public Library, NY
- American University Library, DC
- Santa Clara City Library, CA
- Wayne State University Library

Access by Users

Users have the right to access their own personally identifiable information (PII). The privacy policy should mention this right. Verifying the accuracy and status of PII helps ensure that library services that rely on personally identifiable information can function properly. The right of access covers all types of information gathered about a library user or about his or her use of the library, including mailing addresses, circulation records, computer use logs, etc. Access to personal information should be made available onsite or through secure online access to verify the identity of individual users.

Right to access should also address instances in which age may be a factor. For example, several state library confidentiality grant parents a right to view their minor child's library records, too. The Children's Online Privacy Protection Act of 1998 (COPPA) provides for "a parent's ability to review, make changes to, or have deleted the child's personal information." For more on COPPA, see Part III of "School Libraries" below.

Examples of Access Statements from Sample Library Privacy Policies:

- Duke University
- Boston Public Library
- Multnomah Public Library, OR
- Indiana University

Emerging Technologies with Privacy Concerns

The continuing use of and accelerating dependence on emerging technologies to provide both traditional innovative library services have constituted major challenges for the library profession. It is important for libraries not to take on the attitude that patrons no longer care about privacy. Studies from the Pew (Anonymity, Privacy and Security Online) show the opposite. Patrons may not possess the discursive language or technology terms to articulate their complaint, however, it doesn't mean that they do not care about data harvesting, data mining and sharing of their personal information behind the scenes with third parties. The lack of transparency in consent, data sharing and terms of service changes is a barrier to patron-centered service. It's imperative that libraries understand each new technology by defining them and identifying the mechanism through which each patron's privacy may be breached. As stewards of patrons' data, we owe them the truth and some options. We realize that access to proprietary information and the business model may not be possible in some instances. Through ALA's existing policies we may find that there are already sufficient protections in place, however, there is definitely room for improvement, for the future.

(Definitions are based on: Burke, John. *Neal-Schuman library Technology Companion: A basic* *guide for library staff*. 4th ed. Chicago: Neal-Schuman, ALA, 2013. Print.)

Apps: A piece of software or a program, typically small, that can be used on a computer, smartphone or tablet.

Concerns: Libraries using apps to promote library services or pushing them out to new audiences should be aware that apps log IP, monitor behavior and capture activities. At best, apps are fun, allowing users to gain social status and self-regulate movement. At worst, they can collect highly personal data and post on your libraries behalf with little consent. Companies can then profile a patron or predict behavior based on the information gathered.

Examples: Key Ring, Foursquare, Evernote, Pinterest.

Policy: #B.8.5.2 Confidentiality of Personally Identifiable Information about Library Users.

Camera Surveillance: Cameras monitor, record and archive activities. Mounted on lots, lamp posts and even on patron computers and telephone consoles. Some surveillance cameras may intercept smartphone communications.

Concerns: Libraries choosing to use surveillance cameras in areas where there is reasonable expectation for privacy and parts of the building run the risk of inadvertently violating rights of patrons--adults, minors and students, without just cause. More often, surveillance cameras are not powerful enough to capture concrete data to identify the culprit and puts the library in the business of policing rather than library service.

Examples: Aruba Mesh Network, CCTV, Skyway Security.

Policy: Privacy: An Interpretation of the Library Bill of Right

Cell/Smartphone:

A phone with built-in computer functionality, including e-mail, web browsing and other capacities.

Concerns: Along with its processors, apps and location services comes the ability to measure a user's motion data, track geolocation, following site visits, monitoring social media posts, and snooping on emails.

Examples: Android, Blackberry, iPhone, Google Phone, and Windows Phone.

Policy: #B.2.1.19 Access to Digital Information, Services, and Networks

Cloud computing:

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service); three service models (Cloud Software as a Service (Saas), Cloud Platform as a Service (PaaS), Cloud Infrastructure as a Service (IaaS)); and, four deployment models (Private cloud, Community cloud, Public cloud, Hybrid cloud). Key enabling technologies include: (1) fast wide-area networks, (2) powerful, inexpensive server computers, and (3) high-performance virtualization for commodity hardware. -An excerpt from the definition published in October 2011 by the National Institute for Standards and Technology.

Concerns: As more companies and individuals choose cloud services for convenience or to save money, valid concerns on how secure data can be when they lay in farm servers in remote areas and by a few entities. One's data may reside in a server in a different country, which may implicate questions of legal jurisdiction.

For example, Amazon AWS now holds more than a trillion projects in the cloud. "The trend is that it will become more dominant than desktop computing in the next decade." (Pew Report, 2010).

Examples: AWS, EMC, Skydrive, Google Drive, Apple iCloud.

Policy: #B.2.1.19 Access to Digital Information, Services, and Networks

#B.8.5.2 Confidentiality of Personally Identifiable Information About Library Users

Privacy: An Interpretation of the Library Bill of Rights

e-book (electronic book) and e-periodicals:

An electronic version of a book or periodical that may be read via the web on a computer work station or using a mobile device (e.g., an e-reader, an iPad or a smartphone).

Concerns: Most subscription-based services such as Amazon, Overdrive and Zinio require patron consent to the collection, transfer, manipulation, storage and use of pii. Patrons will need to be aware of how the publishing industry has begun to embrace big data including deep analysis of their digital reading habits like reading speed, how many times they've opened an ebook and other insights into how they're engaging with their book.

Ex. of formats: Standards include epub, kindle, pdf and READ.

Ex. of middleware: Adobe Digital Editions, Amazon Kindle, Overdrive Media Console.

Ex. of tablets: Galaxy, iPad, Kindle, Nook.

Policy: #B.2.3 Freedom to Read.

#B.2.1.19 Access to Digital Information, Services, and Networks.

MOOCs & E-Learning:

MOOCs are Massive Open Online Courses and they are rapidly changing the game for higher education and employee professional development. MOOCs offer free online course covering a growing range of topics delivered by qualified lecturers from some of the well-known universities in the world. They allow a single teacher/lecturer to teach thousands and sometimes tens of thousands of participants in a single course delivery. They are often in an asynchronous course format, using smart phones and mobile computing to connect to the participant.

Concerns: There is concern that students will be tracked. Data breaches, password reuse, identity information and marketing calls can ensue.

Examples: Platform providers include Coursera, EdX and Khan Academy, Udacity and FutureLearn.

Policy: #B.8.5.2Confidentiality of Personally Identifiable Information About Library Users.

Interactive Online Public Access Catalog (OPAC):

The computer version of the card catalog allows an individual to search the holdings of a library through electronic interface. Service can be deployed by SaaS through a patron-discovery interface called Bibliocore (similar to iTune's Tunecore). Some OPACs collaborate with search engines, book apps and third parties. They could possess unlimited user-added tagging features. Others are interactive with social media tools that create booklists, write reviews and gain followers.

Concerns: The lessening of control over patron borrowing records and the lack of discretion for accommodations by library professionals is a concern for intellectual freedom. When libraries no longer retain exclusive authority to their own collections, patron privacy is not directly protectable which makes contract negotiations with third parties even more important. Some OPACs are powered by aggregators like Bibliocore.

Types: Bibliocommons, OCLC.

Policy: #B.4.3 Bibliographic Databases

#B.2.1.19 Access to Digital Information, Services, and Networks

Radio Frequency Identification (RFID):

A method used by libraries to protect their physical collections by placing a small tag on each item; tag consists of a computer chip with antenna attached, and security gates or self-checkout systems can then read the tag to complete their functions. Although RFIDs have been existence since the late 1990s, types of RFID can be considered emerging technology.

Near Field Communication (NFC):

NFC is a short-range, standards-based, contactless connectivity based on RFID technology that uses magnetic field induction to enable communication between electronic devices in close proximity. For two devices to communicate, one device must have an NFC reader/writer and the other has to have an NFC tag. http://www.nearfieldcommunication.org/about-nfc.html

Concerns: NFC library cards allow patrons to pay for fines, books and unlock print jobs using Google Wallet, ISIS, PayPal, using an NFC-enabled smartphone or a laptop. Tags can hold up to 1 MB of information and are embeddable in books, posters, etc.

Types: NFC, HF, UHF

Policy: ALA/RFID in Libraries Privacy and Confidentiality Guidelines

Social Networking Tools:

Social networking tools allow people to bond online and chat, exchange pictures and videos and stay connected through a medium they use daily. People join the networks, post as much or as little personal information as they would like, connect with the people they already know in daily life, add on new virtual friends drawn from shared interests, or locate and reconnect with old friends who are geographically distant. Each library setting will need to find a balance between just being present and actively sharing in a social networking site.

Concerns: Without careful curation, privacy will be compromised. Libraries will have to find a careful balance between information dissemination and user privacy in each individual situation.

Types: Facebook, Skype, Twitter, Tumblr and YouTube.

Policy: #B.2.1.19. Access to Digital Information Services and Networks

#B.2.2 Freedom to View

At the time of writing, the above were the most prevalent emerging technologies. By no means is this list exhaustive. It's impossible to predict which companies will merge and change the terms of privacy or what third party vendors will take over the development of a product. What we can do is remember that it is important for libraries and librarians to continue to treat patron information with due care and consideration. Emerging technologies are changing social norms regarding privacy, providing new avenues for compromising rights. Libraries need to keep up-to- date on the developments and librarians need to remain vigilant.

References:

Downes, Stephen. "Moocs and k12 Cloud: Privacy regulations and Risk Management." *Slide Share*. National Research Council Canada, 03 May 2013. Web. 26 Dec 2013.

Ryan, Dr. Lindsay. "White Paper: MOOCs-Massive Open Online Courses." EFMD, n.d. Web. 7 Jan 2014.

Vacca (ed), John R. Computer and Information Security Handbook, Second Edition. Morgan Kaufmann Publishers, © 2013. Books24x7. Web. Dec. 2, 2013.

Data Integrity & Security

Data Integrity: The library needs to assure data integrity. Whenever personally identifiable information (PII) is collected, the library must take reasonable steps to ensure integrity, including using only reputable sources of data, providing library users access to their personal data, updating information regularly, destroying untimely data or converting it to anonymous form, and stripping PII from aggregated, summary data. The library staff is responsible for destroying information in confidential or privacy- protected records to ensure against unauthorized disclosure. Information that should be regularly purged or shredded includes PII on library resource use, material circulation history, security/surveillance tapes, and both paper and electronic use logs.

Shared Data: If patron records are supplied by or shared with a parent institution such as a college registrar or a library consortium, the library needs to adopt measures to ensure timely corrections and deletions of data. Likewise, when the library exchanges data with other departments such as bursars and tax collectors, vendors, or any other organizations, it must ensure that records are accurate and up to date. Libraries issuing passwords should avoid choosing passwords or PIN's that can reveal a user's identity, including social security numbers.

Big Data—data aggregation and analytics: Shared endorsement settings, mash-ups that combine services to create an entirely new service may reduce redundancy, spare users from typing and repurposing data may be desirable for data management efficiency. Libraries may look at combined services because it's easier. The disadvantage is that it's too easy to make incorrect correlations when personally identifiable information sits side by side with other data. Unless a patron opts-in, reading records should never be correlated with patron conduct, database usage, meeting room signups, etc. Libraries should also be aware of what information may be publicly visible. Data may exchange many hands with third parties, using libraries as conduits, allowing more opportunity for privacy breaches and data mining. As stewards of patron privacy, libraries should steer away from the practice of creating aggregate data without legitimate purposes.

Security: Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of data. Security measures should be integrated into the design, implementation, and day-to-day practices of the library's entire operating environment as part of its continuing commitment to risk management. This should include the guarantee of a secure wireless network for patrons to use. These measures are intended to prevent corruption of data, block unknown or unauthorized access to library systems and information, and provide reasonable protection of private information in a library's custody, even if stored offsite on servers or backup tapes.

Administrative Measures: The library needs to implement internal organizational measures that limit access to data while ensuring that individuals with access do not utilize the data for unauthorized purposes. The library must also prevent unauthorized access by using technical security measures like encrypting transmitted and stored data, limiting access by using passwords, and storing data on secure servers or computers inaccessible by modem or network. If libraries store PII on servers or backup tapes offsite, they must ensure that comparable measures to limit PII access are followed. Libraries should also develop routine schedules for shredding PII collected on paper.

Electronic Tracking: Neither local nor external electronic systems used by the library should collect PII through logging or tracking e-mail, chat room use, Web browsing, cookies, middleware, or other technology usage. Nevertheless, users should be advised of the library's privacy protection limits when using remote sites. If the library enables cookies (small files sent to a browser by a Web site to enable customization of individual visits), it should instruct users on how to refuse, disable, or remove cookies from their hard drives. Moreover, the library should not maintain cookies after users terminate their sessions or share them with external third parties. Libraries should regularly remove cookies, Web history, cached files, or other computer and Internet use records and other software code that is placed on their networks. Those libraries that authenticate patrons for use of external databases by middleware systems and/or proxy servers should simply verify the attributes of valid users and not release PII.

Data Retention: It is the responsibility of library staff to destroy information in confidential or privacy- protected records in order to safeguard data 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. If this data is maintained off-site, library administrators must ensure that appropriate data retention policies and procedures are employed. Libraries that use surveillance cameras should have written policies stating that the cameras are not to be used for any other purpose. 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.

Encryption: The use of data encryption can help enhance privacy protection. Encrypted data requires others to use a pre-defined electronic key to decipher the contents of a message, file, or transaction. Libraries should negotiate with vendors to encourage the use of such technology in library systems (e.g., in the document delivery, saved searches, and e-mail 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.

Selected Links:

- ALA Task Force on Privacy and Confidentiality in the Electronic Environment. Final Report.
- California Digital Library, SOPAG Privacy Audit and Guidelines
- Center for Democracy and Technology, Authentication Privacy Principles Working Group
- CERT Tech Tips
- Cookie Central, Frequently Asked Questions About Cookies
- Electronic Frontier Foundation, Privacy, Security, Crypto, & Surveillance
- The Electronic Privacy Information Center, Cookie Page
- The Electronic Privacy Information Center, International Data Retention Page
- International Coalition of Library Consortia, Privacy Guidelines for Electronic Resources Vendors
- IEEE, Security & Privacy Magazine
- The Shibboleth Coalition
- World Wide Web Consortium, The World Wide Web Security FAQ: 8. Server Logs and Privacy

Examples of Retention Schedules from Sample Library Privacy Policies:

- Library of Virginia
- Texas State Library and Archives Commission

- Ohio State University Libraries
- University of Michigan Library

Examples of Security Statements from Sample Library Privacy Policies:

- Cleveland Heights-University Heights Public Library
- Duke University Library
- John Carroll University Library
- Seattle Public Library
- Syracuse University Library

Enforcement & Redress

Libraries that develop privacy policies need to establish and maintain an effective mechanism to enforce them. They should conduct regular privacy audits to ensure that all library programs and services are enforcing these policies. Redress must be available for library users who feel their privacy and confidentiality rights are violated. Libraries should provide a means to investigate complaints and re-audit policy and procedures in cases of potential violation of library privacy and confidentiality. Library educational efforts should include informing users how to protect their own privacy and confidentiality, both in and outside of the library setting.

Selected Links:

- ALA Office for Information Technology Policy, Top tips for Protecting Privacy Online
- United States Federal Trade Commission, Privacy & Security

Government Requests for Library Records

Libraries must ensure they have well-established procedures to enforce their policies by informing users about the legal conditions under which they might be required to release personally identifiable information (PII). Libraries should only consider a law enforcement request for any library record if it is issued by a court of competent jurisdiction that shows good cause and is in proper form. Only library administrators, after conferring with legal counsel, should be authorized to accept or comply with subpoenas, warrants, court orders, or other investigatory documents directed to the library or pertaining to library property. All library staff should be trained and required to contact a designated Library Privacy Officer or previously designated administrator immediately should a law enforcement officer appear requesting library compliance with a request to release PII.

Libraries should develop and implement procedures for dealing with law enforcement requests before, during, and after a visit. Guidance on these matters can be found in the following ALA documents:

- Confidentiality and Coping with Law Enforcement Inquiries: Guidelines for the Library and Its Staff, April 2002
- Suggested Procedures for Implementing Policy on Confidentiality of Library Records (http://www.ala.org/offices/oif/statementspols/otherpolicies/suggestedprocedures), 1988
- USA PATRIOT Act (http://www.ala.org/advocacy/advleg/federallegislation/theusapatriotact)
- Guidelines for Librarians on the USA PATRIOT Act: What to do before, during and after a "knock at the door?" http://www.ala.org/advocacy/sites/ala.org.advocacy/files/content/advleg/federallegislation/theusapatriotact/patstep.pdf), January 2002

To learn more about federal search and seizure guidelines, see:

- United States Department of Justice Criminal Division Computer Crime and Intellectual Property Section, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf), July 2009

Examples of Disclosure/Court Order Statements from Sample Library Privacy Policies:

- Fort Vancouver Regional Library District (http://66.96.75.5/aboutus/policies/confidentiality.htm)
- Kansas City Public Library (http://www.kclibrary.org/000-internal-policies)
- Madison, WI, Public Library (http://www.madisonpubliclibrary.org/policies/confidentiality-library-records)
- Mansfield, OH (http://www.mrcpl.org/pages/about-us/policies/public-records-policy)
- Queensboro Public Library (http://www.queenslibrary.org/about-us/privacy)
- College of St. Catherine http://libguides.stkate.edu/content.php?pid=320766&sid=2625435#11931643)
- Indiana University - Purdue (http://www.ulib.iupui.edu/libinfo/privacy)
- Vanderbilt University (http://www.library.vanderbilt.edu/policies/privacy.php)

Special Privacy Policy Considerations

Academic Libraries

The Freedom to research unfamiliar and controversial topics is central to the mission of academic institutions. Academic libraries serve those needs well. They frequently provide their personal, professional, and educational information services to a wide variety of users. If academic libraries provide different levels of service or access to different categories of borrowers (e.g., faculty, graduate students, undergraduate students, or community members), they must ensure that their services and access are offered equitably within a borrower type. Such restrictions should not impede intellectual freedom.

Academic Libraries and Students: Students in academic institutions are adults and must be accorded the same privacy safeguards as adults in other types of libraries. The mere fact that students are enrolled in courses should not jeopardize their privacy rights. Thus, student circulation records for course-required and reserve reading should be protected from inquiry with the same rigor as their circulation records for personal reading. Librarians assisting in investigations of plagiarism should take care to protect the usage records of individual students. Librarians can assist faculty in the development of classroom instruction and procedures that meet educational goals without compromising student rights to privacy.

Academic Libraries and FERPA and SEVIS: The Family Educational Rights and Privacy Act (FERPA) was passed to protect the privacy of student education records and to define who can access these records. FERPA grants parents the rights until the child turns 18 years old or attends a school beyond the high school level. At the age of 18 or when students attend institutions of higher learning, they assume the right to access and protect the privacy of their educational records. The Student and Exchange Visitors Information System (SEVIS) maintains updated information on approximately one million non-immigrant foreign students and exchange visitors during the course of their stay in the United States each year. Colleges and universities are now required to report a foreign student's failure to enroll or if students drop out of their programs. Colleges and university librarians need to identify how their institutions implement these laws and whether they have any impact on the collection and retention of library user records.

Academic Libraries and Faculty: Academic institutions often rely on principles of academic freedom to protect the intellectual freedom of faculty. While the principles of academic freedom are intended to protect faculty from professional consequences of researching unpopular or controversial areas, they do not necessarily protect the privacy of faculty. Academic libraries should also have in place appropriate policies based on First Amendment and Fourth Amendment rights to protect the privacy of faculty members' library records.

Academic Libraries and Computer Systems: The computer networks of academic libraries are often part of institutional networks, under the ultimate control of units outside the library. Academic libraries should work with campus computer departments to ensure that student and faculty information-seeking activity is kept confidential and well protected throughout the institution. In addition, library personnel should review library procedures and arrangements with outside vendors to ensure the highest level of protection for such records as online digital reference logs, proxy server and other authentication devices, e-mail reference transactions, personalized searching, and SDI profiles.

Selected Links:

- Cause, Privacy and the Handling of Student Information in the Electronic Networked Environment of Colleges and Universities, 1997
- American Library Association, Intellectual Freedom Principles for Academic Libraries: An Interpretation of the Library Bill of Rights
- Barbara M. Jones, "Academic Libraries and Intellectual Freedom"
- United States Department of Education, Family Educational Rights and Privacy Act [FERPA]
- United States Department of Education, Protecting the Privacy of Student Records, Guidelines for Education Agencies
- United States Department of Homeland Security, SEVP: Student and Exchange Visitor Program
- Virginia Rezmierski and Nathaniel St. Clair, II, Identifying Where Technology Logging and Monitoring for Increased Security End and Violations of Personal Privacy and Student Records Begin: Final Report NS-LAMP Project, Washington, DC: American Association of Collegiate Registrars and Admissions Officers, 2001

School Libraries

School librarians have an ethical obligation to protect and promote student privacy. Although the educational level and program of the school necessarily shapes the resources and services of a school library, the principles of the Library Bill of Rights apply equally to all librarians, including school librarians. School librarians are in a unique position to educate students & staff about the implications of sharing information with others as well as the library's role in protecting privacy.

School Libraries and FERPA: "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 disclosure 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. Therefore, school libraries may 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. (ALA Questions and Answers on Privacy and Confidentiality, #33, http://ifmanual.org/privacyqa).

Protecting Students Privacy in a School Library

School librarians have a responsibility to "assume a leadership role in promoting the principles of intellectual freedom within the school by providing resources and services that create and sustain an atmosphere of free inquiry." This includes safeguarding student and teacher privacy. School library personnel must strive to: educate all members of the school community about the value of school library users; develop board approved policies that provide the highest level of protection for all records; and teach all members of the educational community about the policies and procedures that govern privacy. School libraries operate as part of larger educational structures. In some cases school systems may create policies and procedures that infringe on students' rights to privacy. School library personnel are encouraged to educate all policy makers about the dangers of abridging students' privacy rights.

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, ti 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. See: ALA Questions and Answers on Privacy and Confidentiality.

Educating Students and Staff about Privacy: In addition to protecting patrons' privacy, school librarians play a vital role in educating faculty, staff and students about privacy. We live in an era when personal information is widely available online, and online networks and databases collect and store personal information. These facts present growing challenges to individuals' privacy. Students need to be aware of the implications of their online activities in terms of personal safety, identity safety, and security of future academic and employment opportunities. School Librarians should educate students to engage in online communication and interaction that is responsible, ethical and safe. For this purpose, ALA has developed ideas, tools and resources specifically for school libraries available through their Choose Privacy site (www.chooseprivacyweek.org).

School libraries and COPPA:

School libraries and COPPA: The Children's Online Privacy Protection Act (COPPA) regulates commercial Web sites and online services, including apps, which are directed to children under the age of 13 and collect children's personally identifiable information, as well as general audience sites that know they are collecting personally identifiable information from children 13 and under. Such sites have a legal obligation to comply with the law. Operators who violate COPPA can be held liable for civil penalties of up to $16,000 per violation by the Federal Trade Commission (FTC) the agency responsible for enforcing COPPA.

Noncommercial Web sites, such as library, nonprofit, community groups, and government agencies are not subject to COPPA. A library collecting personal information from children in order to e-mail them summer reading lists or reference assistance is not required to seek parental consent. However, libraries should be aware that changes to the COPPA rules adopted in December 2012 require any site that integrates outside services, such as plug-ins, apps, or advertising networks that collect personal information from site visitors to comply with COPPA if the site operator knows that the outside service is collecting information from children under 13. A library should carefully review any app or outside service's data collection practices before integrating it into its website.

Although libraries are not directly impacted by COPPA, children using the Internet in a library may need help understanding the law and getting consent from their parents to use websites and apps. In some instances, children will find that COPPA may restrict their ability to participate in some activities on Web sites while they await parental approval. It is the librarians' role to guide children through the process or help them find alternative activities online. Parents may need assistance in understanding the law and the significance of the requests they receive from Web sites.

Librarians and libraries should play a key role in helping all library users understand and comply with COPPA. (Note: The extent to which schools can or do assume parental responsibilities for students will depend in large part on decisions made by the local school board or superintendent. It will also depend on the nature of the resources being used in the classroom and whether those resources require students to divulge personally identifiable information. Some schools may decide to act on behalf of the child, others may decide to seek consent although an Acceptable Use Policy signed by students and parents at the beginning of the year, while others may take no responsibility at all and leave it up to parents. However the school implements the law, it must take care not to allow COPPA to interfere with curricular decisions.)

Selected Links:

- American Association of School Librarians, Position Statement on the Confidentiality of Library Records
- American Library Association. Minors and Internet Interactivity: An Interpretation of the Library Bill of Rights.
- Family Educational Rights and Privacy Act (1974) information
- Privacy Resources for Librarians, Library Users, and Families
- State Privacy Laws Regarding Confidentiality of Library Records

- United States Department of Education, Family Policy Compliance Office Web Site
- Legal Information Institute, Family educational and privacy rights from the US Code

Public and Academic Library Services to Minors

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. Furthermore, the legal responsibilities and standing of library staff in regard to minors differ substantially in school and public libraries. In all instances, best practice is to extend to minors the maximum allowable confidentiality and privacy protections.

The Children's Online Privacy Protection Act (COPPA) requires commercial Web sites and online services that collect personally identifiable information from children 132 and under to obtain consent from their parents or guardians in advance. (Please see the detailed information about COPPA in the section on school libraries.) Although COPPA does not usually place any special obligations on public libraries, there are two impacts to consider:

1. When children use internet access in libraries, library staff need to be able to explain COPPA's effects to children and their parents.
2. When a library designs Web pages and services for children, it may wish to provide the same privacy protections as the protections mandated for commercial Web sites.

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 minor children about those choices. Librarians should not breach a minor's confidentiality by giving out information readily available to the parent from the minor directly. Libraries should take great care to limit the extenuating circumstances in which they release such information.

Parental responsibility is fundamentally important 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.

The Minors’ right to privacy regarding their choice of library materials should be respected and protected.

Selected links:

- YALSA website
- Minors' Rights to Receive Information Under the First Amendment
- Complying with COPPA: Frequently Asked Questions

ASCLA Statement of Privacy Rights

The Association of Specialized and Cooperative Library Agencies asserts the fundamental position that a right to privacy exists equal for all people regardless of physical, psychological, intellectual, social, or political condition.

In providing service to special populations, librarians, support staff, and other service providers must be aware of that fundamental right to confidentiality of materials and records and take affirmative action within the institutional structure to maintain these privacy rights.

ASCLA Board of Directors, adopted January 27, 2014

Implementation of Privacy Policies and Procedures

Responsibilities of Governance Bodies/Policy Makers

- Be informed about issues relating to library patron and user privacy and confidentiality, including those specific to minors.
- Be aware of applicable federal, state and local laws and regulations.
- Adopt appropriate policies related to patron privacy and library record confidentiality.
- Understand the library's or educational institution’s plan for routine and crisis communication.
- Be knowledgeable about techniques for dealing with the media.

Responsibilities of Directors/supervisors

- Remain informed regarding issues relating to library patron and user privacy and confidentiality including K-12 students and minors in other library settings.
- Be knowledgeable about applicable federal, state and local laws and regulations.
- Inform and educate policy making bodies regarding relevant professional, ethical and legal issues related to patron privacy.
- Recommend privacy and confidentiality policies to policy makers consistent with professional core values, the Code of Ethics, and applicable law.
- Ensure all contracts with ILS (integrated library system) and other vendors are

consistent and compliant with the library's privacy policies.

- Ensure that contracts for fee-based databases offer anonymous searching.
- Conduct privacy audits to review and evaluate current policies, practices, and procedures.
  - Identify the type and nature of all records and files containing library patron and user personally identifiable information.
- Develop guidelines and procedures in support of policies:
  - Define patron privacy and confidentiality.
  - Incorporate privacy issues and protections into relevant library policies.
  - Establish a schedule for the retention of records and files containing library patron and user personally identifiable information.
  - Create a chart of the library's organizational hierarchy, indicating:
    - Chain of command.
    - Staff members authorized to respond to requests for patron or user personally identifiable information.
- Define and describe the type and nature of requests for personally identifiable information:
  - Informal requests for patron records
    Determine the circumstances under which, the manner of and extent to which patron and user personally identifiable information may be disclosed in person, over the phone or electronically. In school and academic libraries, be mindful of the guidelines under the Family Educational Rights and Privacy Act (FERPA) for release of student library records.
  - Law enforcement requests for patron records
    Detail the specific steps staff should follow in responding to investigatory requests for patron and user personally identifiable information from:
    - Local and state agencies
    - Federal agencies including FISA/PATRIOT Act requests/orders
- Write a ready-reference card with a clear and concise description of the library's privacy policies.
- Designate a library staff member to serve as the Library Privacy Officer who will:
  - Monitor news and information about privacy issues.
  - Train library staff on privacy and confidentiality issues, policies, and procedures: Specify the staff response process to public, media, or law enforcement requests for library patron and user personally identifiable information.
  - Develop a routine crisis communication plan in relation to privacy practices

and privacy inquiries.
    - Designate a library or educational institution spokesperson(s).
    - Educate the public as well as the school board, school administrators, teachers, students, and parents about issues of library privacy and confidentiality and the library's policies, practices and procedures.
    - Maintain contact with local, regional and national affinity organizations.
    - Forge alliances with community groups.

Responsibilities of Staff

- Maintain privacy and confidentiality when assisting library patrons and users taking special care with minors.
- Discuss matters of library patron and user personally identifiable information with other staff only in non-public areas and when necessary for operational purposes.
- Refer all requests for access to, or view of, non-public computers, files or records to a library or school district administrator.
- Keep confidential the source of any request or the nature of the information requested.

Responsibilities of Information Technology Services Staff

- When considering emerging technologies, write a viable technology plan which can evolve with third party vendor updates yet remain firm in protecting patron privacy
- Consider patron privacy in any RFP (Request for Proposal) bid, query, service or project.
- Ensure all contracts with ILS (integrated library system) and other vendors are consistent and compliant with the library's policies
- Ensure ITS staff understand patron rights to privacy and confidentiality remains critical when transitioning to a virtual environment or purchasing new software
- Prominently post or articulate to the patron any instance where patron privacy is no longer being maintained by the library system (eg: leaving the library’s website to enter a third party database)
- When evaluating technology, ask whether it has been successful in protecting patron privacy or were there loopholes in breaching privacy which may require attention

Library Privacy Talking Points: Key Messages and Tough Questions

In an age of “sound bites” in which media may only provide to ten to fifteen seconds for a response, the ability to provide succinct yet coherent responses to tough question is crucial. This section provides language suitable for use in public settings to provide those concise answers.

Key Messages

- Privacy is essential to the exercise of free speech, free thought and free association.
- Libraries are a cornerstone of democracy and help ensure Americans are able to read, research, and think freely.
- Forty-eight states and the District of Columbia have statutes declaring library records as confidential documents. The two remaining states, Hawaii and Kentucky, have opinions issued by their attorneys general finding library records to be confidential documents. See State Privacy. "The library community recognizes that children and youth have the same rights to privacy as adults." AASL "Position Statement on the Confidentiality of Library Records."
- Librarians have always cooperated with law enforcement within the framework of state and federal laws and regulations.
- Librarians have a responsibility to protect the privacy and confidentiality of our patrons while responding to legitimate national security concerns

Tough Questions about Library Privacy – with answers

Why do libraries protect the confidentiality of library reading records?

- Forty-eight states and the District of Columbia have statutes declaring library records as confidential documents. The two remaining states, Hawaii and Kentucky, have opinions issued by their attorneys general finding library records to be confidential documents.
- States created these confidentiality laws to protect the privacy and freedoms Americans hold dear. These laws provide a clear framework for responding to national security concerns while safeguarding against random searches, fishing expeditions or invasions of privacy.
- Laws protecting the confidentiality of library records help to assure that no person comes under suspicion simply because he or she reads a disapproved book, or does research into a disapproved topic. Reading about chemistry does not make a person a terrorist bomber, nor should reading about childbirth and parenting place you under suspicion for abandoning an infant.
- With or without specific legislation, school librarians [and youth librarians] are urged to respect the rights of children and youth by adhering to the tenets expressed in the ALA Policy on Confidentiality of Library Records, Privacy: An Interpretation of the Library Bill of Rights, ALA Code of Ethics." and the AASL Position Statement on the Confidentiality of Library Records. Lack of privacy can be harmful to minors if reading interests are exposed when help is sought from domestic crisis or abusive authority figures.

Additionally, reading privacy is important for affirming identity, understanding self-development and overall health. Article Sixteen of the United Nations Convention on the Rights of the Child

- Librarians maintain records to ensure the efficient operation of the library, not to review or document individuals' reading habits. Libraries do not keep or maintain print or electronic records as a means of law enforcement.
- It is standard practice that libraries do not create nor maintain unnecessary records. In fact, this is such a common practice that integrated library systems (ILSs), the software that helps libraries manage their collections and maintain borrowing records, are designed to support records retention for only as long as required for efficient operation of the library. Borrower information is erased from database in a timely manner.
- As vendors of ILSs continue to move toward cloud-based installations libraries should make every effort to work with these vendors to retain all patron information on local servers to insure the privacy and confidentially of their patrons.

What is ALA's position on the confidentiality of library records when sought by law enforcement officers?

- The ALA encourages libraries to put in place procedures for working with law enforcement officers when a subpoena or other legal order for records is made. Libraries will cooperate expeditiously with law enforcement within the framework of the law.
- If librarians do not follow state confidentiality laws and legal procedures, they run the risk of actually hurting ongoing police investigations. The American judicial system provides the mechanism for seeking release of confidential records: the issuance of a court order, showing probable cause based on specific facts and in proper form.
- The USA Patriot Act expanded the FBI’s power to obtain material from businesses and libraries related to counterterrorism and anti-espionage investigations. The intersection of federal and state privacy laws is a complicated matter and needs to be decided on a case-by-case basis.

Why does the American Library Association oppose certain provisions of the USA PATRIOT Act?

- Librarians, like all Americans, are concerned about terrorism and the safety of our families and friends; however, the threat of terrorism must not be used as an excuse to intrude on our basic constitutional rights. We can fight terrorism, but we can do it at the same time as we protect our civil liberties.
- The American Library Association is concerned about the provisions of the USA PATRIOT Act that allow the FBI to seek information on Americans' reading habits, as if it were possible to determine what someone might do based on what he or she has read. USA

Patriot Act: Advocacy Legislation & Issues

- Section 215 of the PATRIOT Act greatly expanded the FBI's ability to get records from all businesses, including libraries and booksellers, without meeting the traditional standard needed to get a search warrant in the United States.
- The PATRIOT Sunset Extension Act of 2011, signed into law on May 26, 2011 included four (4) extensions of three key provisions of the USA Patriot Act: roving wiretaps, searches of business records (the "library records provision"), and conducting surveillance of "lone wolves"—individuals suspected of terrorist-related activities not linked to terrorist groups.
- The ALA supports amendments to the USA PATRIOT Act that would strengthen the protection of the right to read and pursue information without fear of government surveillance as well as active oversight of the implementation of the USA PATRIOT Act.
- The American Library Association encourages all librarians, library administrators, and library advocates to educate their communities about the process for compliance with the USA PATRIOT Act and other related measures and about the dangers to individual privacy and the confidentiality of library records resulting from those measures.

How should libraries respond to requests for records under the US PATRIOT Act?

- Individual libraries may not be at liberty to discuss the specifics of any legal search because a gag order accompanies a search warrant or subpoena issued under the USA PATRIOT Act.
- The ALA recommends that libraries seek legal counsel to ensure proper handling of National Security Letters (NSL). They are documents signed by officials of the FBI and other agencies, without prior judicial approval, which compel disclosure information. NSLs are usually accompanied with a gag order, prohibiting disclosure of the fact or nature of the request. An amendment included in the USA Patriot Act Additional Reauthorizing Amendment of 2006, signed in to law in February of 2006 allows for sharing the information with the library's lawyer.

What is ALA doing

The American Library Association:

- creates and updates policies and procedures about privacy and confidentiality. See Privacy and Confidentiality
- represents libraries in federal policy making and court proceedings.
- develops tools to help libraries ensure privacy and confidentiality for all users and staff.
- works with other organizations concerned with free expression and privacy concerns. See First Amendment Advocates

- monitors developments in the privacy arena.
- assists libraries with legal action.
- provides guidance and other assistance when library privacy is challenged.
- advocates for the public's rights to access information, enjoy free expression, and privacy.
- provides specific guidance related to the Children's Online Privacy Protection Act. See Bureau of Consumer Protection: Children's Privacy
- advocates through its divisions—AASL, ALSC, and YALSA— for privacy of minors in their position statements, publications, and online presence.
- Sponsors the annual Choose Privacy Week observation during the first week in May.

Advocacy at the Local, State, & National Levels

You and your library or institution should:

- keep informed, monitor, and advocate for legislation that protects user privacy by contacting elected officials
- Link to ALA's Washington Office for
    - Information about pending legislation and potential impact on libraries.
    - ALA resolutions that support or oppose legislative actions.
    - Bill status.
- Link to the Office for Intellectual Freedom for privacy resources.
    - Information about privacy and the impact of various legislative and judicial action on free expression. See American Library Association Privacy Policies and Statements
    - The Privacy Tool Kit (2014)
    - ALA resolutions reaffirming the principles of intellectual freedom and confidentiality of library records.
    - Privacy: An Interpretation of the Library Bill of Rights
    - State Privacy Laws Regarding Library Records
    - Confidentiality and Coping with Law Enforcement Inquiries: Guidelines for the Library and its Staff
- Link to Freedom to Read Foundation for
    - Information from the Freedom to Read foundation which is particularly interested in protecting patron privacy and curtailing expanded government surveillance powers in libraries and bookstores.
- contact legislators at the federal, state, and local levels to persuade lawmakers to amend and change laws that infringe on civil liberties.
    - Attend National Library Legislative Day sponsored by ALA and DCLA

    - Attend your state legislative day.
    - Establish a personal relationship with your federal, state and local legislators and staff.
    - Write letters and include resolutions passed by your professional organization
    - Hold law enforcement agencies accountable.
    - Ask local law enforcement officials to speak to local organizations, town meetings and participate in programs at your library.
    - Keep abreast of local law enforcement activities concerning civil liberties and privacy.
    - Keep informed about court cases such as the denial of Freedom of Information Act requests for information about surveillance of library users.
- educate library and school boards and staff, communities, media, and local governments by:
    - Publicizing the need for libraries to adopt privacy policies.
    - Proposing the creation of a Privacy Officer whose duties would include ensuring institutional rules and procedures to promote and confidentiality.
    - Writing newspaper articles, guest editorials, and letters to the editor.
    - Making presentations to local and civic organizations.
    - Keeping local government officials up to date on privacy issues.
    - Gathering information about impact on local communities by compiling Web site links concerning the effects of laws and governmental actions that infringe on civil liberties and privacy.
    - Inviting privacy specialists to speak and conduct workshops.
- organize a publicity campaign.
    - Prepare brochures and handouts to explain local and national impacts.
    - Take out ads in local newspapers.
    - Organize town meetings and public forums.
- form or join coalitions.
    - Develop alliances with other groups advocating for privacy rights.
    - Cooperate with other interested organizations like the ACLU, AAUW, League of Women Voters, Common Cause, religious and civic groups, and local bar associations in discussions about how to counter the sections of laws that infringe on civil liberties.
    - Make your community a "Civil Liberties Safe Zone." See the Bill of Rights Defense Committee.
    - Make information available to those, such as library boards and organizations, local governmental bodies and others, who want to pass resolutions opposing laws that infringe on civil liberties (or parts of them) and related matters.

- Urge libraries to join court challenges.
  - Investigate appropriateness of joining other groups' initiated court challenges.
  - Keep informed about court cases such as the denial of Freedom of Information Act requests for information about surveillance of library users.

Appendices

Appendix A: Privacy Policy Documents

American Library Association Privacy Policies and Statements

The American Library Association has developed policies, guidelines, and resources to assist librarians in preserving privacy and confidentiality for library users.

Basic Statements

Code of Ethics (rev. 2005) http://www.ala.org/advocacy/proethics/codeofethics/codeethics

Freedom to Read Statement (1953; rev. 1972, 1991, 2000)
http://www.ala.org/advocacy/intfreedom/statementspols/freedomreadstatement

Freedom to View Statement (1990)
http://www.ala.org/advocacy/intfreedom/statementspols/freedomviewstatement

Library Bill of Rights (1948, amended 1961, 1980, reaffirmed 1996)
http://www.ala.org/advocacy/intfreedom/librarybill/

Principles for the Networked World (2002)
http://www.ala.org/offices/sites/ala.org.offices/files/content/oitp/publications/issuebriefs/principles/principles.pdf

Privacy and Confidentiality Policies, Procedures and Statements

ALA Task Force on Privacy and Confidentiality in the Electronic Environment Final Report (July 2000)
http://www.ala.org/lita/about/taskforces/dissolved/privacy

Conducting a Privacy Audit
http://www.ala.org/offices/oif/iftoolkits/toolkitsprivacy/guidelinesfordevelopingalibraryprivacypolicy/guidelinesprivacypolicy#privacyaudit

Materials for Conducting a Privacy Audit
http://www.ala.org/offices/oif/statementspols/otherpolicies/privacyaudit

Guidelines for Developing a Library Privacy Policy (August 2003; rev. March 2005)
http://www.ala.org/offices/oif/iftoolkits/toolkitsprivacy/libraryprivacy

Model Library Policy
http://www.ala.org/offices/oif/iftoolkits/toolkitsprivacy/libraryprivacy#modelprivacy

Policy concerning Confidentiality of Personally Identifiable Information about Library Users (1991)
http://www.ala.org/advocacy/intfreedom/statementspols/otherpolicies/policyconcerning

Policy on Confidentiality of Library Records (1971; rev.1975, 1986)
(http://www.ala.org/Template.cfm?Section=otherpolicies&Template=/ContentManagement/ContentDispl ay.cfm&ContentID=13084)

Suggested Procedures for Implementing Policy on Confidentiality of Library Records (1983; rev. 1988 and March 18, 2005. http://www.ifmanual.org/implementconfidentialitypolicy

American Association of School Libraries. "Position Statement on the Confidentiality of Library Records" (Revised 02/06/12)
http://www.ala.org/aasl/advocacy/resources/position-statements/library-records

Privacy: An Interpretation of the Library Bill of Rights (2002)
http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy

Privacy Resources for Librarians, Library Users, and Families (last updated 2002)
http://www.ala.org/advocacy/privacyconfidentiality/privacy/privacyresources

Questions and Answers on Privacy and Confidentiality (June 19, 2002; rev. April 14, 2005; June 26, 2006; and October 30, 2006) (http://www.ala.org/oif/policies/interpretations/privacyqanda)

Policies and Statements about the Patriot Act and Law Enforcement Inquiries

U.S.A. Patriot Act & Libraries
Including links to statements by other library and civil liberties organizations
http://www.ala.org/advocacy/advleg/federallegislation/theusapatriotact
http://www.districtdispatch.org/?s=Patriot+Act&submit=Go
http://www.ala.org/Template.cfm?Section=ifissues&Template=/ContentManagement/ContentDisplay.cfm&ContentID=32307
(http://www.ala.org/ala/oif/ifissues/usapatriotactlibrary.htm)
http://ifmanual.org/resolutionuseandabuse

Confidentiality and Coping with Law Enforcement Inquiries: Guidelines for the Library and its Staff (last updated 2004) http://www.ala.org/offices/oif/ifissues/confidentiality

FBI in Your Library http://www.ala.org/offices/oif/ifissues/fbiyourlibrary

Resolution on the USA Patriot Act and Related Measures That Infringe on the Rights of Library Users (CD #20.6 2005 ALA Annual Conference)
http://www.ala.org/offices/sites/ala.org.offices/files/content/wo/reference/colresolutions/PDFs/062905-CD20.6.pdf

Other ALA Privacy Related Resolutions

American Association of School Librarians. Position Statement on the Confidentiality of Library Records, (2/6/2012). http://www.ala.org/aasl/advocacy/resources/position-statements/library-records

Loyalty Oaths, (July 1, 1992) http://ifmanual.org/loyaltyoaths

Resolution on Privacy and Standardized Driver's Licenses and Personal Identification Cards, January 19, 2005
http://ifmanual.org/resolutionpsdlpid

Resolution on the Terrorism Information Awareness Program (June 25, 2003)
http://ifmanual.org/resolutiontiap

Resolution on the Need for Reforms for the Intelligence Community to Support Privacy, Open Government, Government Transparency, and Accountability July 2, 2013
http://www.oif.ala.org/oif/?p=4803

Resolution on the Use and Abuse of National Security Letters; On the Need for Legislative Reforms to Assure the Right to Read Free of Government Surveillance (June 27, 2007)
http://ifmanual.org/resolutionuseandabuse

Resolution Reaffirming the Principles of Intellectual Freedom in the Aftermath of Terrorist Attack, (January 23, 2002) http://ifmanual.org/resolutionreaffirm

Resolution to Commend the John Does of the Library Connection, (June 28, 2006)
http://ifmanual.org/resolutionjohndoes

Resolution to Protect Library User Confidentiality in Self-Service Hold Practices (July 5, 2011)
http://www.oif.ala.org/oif/?p=2371

Types of Law Enforcement Requests and Court Orders

Sample federal subpoena, trap/trace, preservation orders, etc.
http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf pp.209 – 264

Search and seizure federal courts
http://www.uscourts.gov/uscourts/FormsAndFees/Forms/AO093.pdf
Sample Federal Search Warrants and Subpoenas

Subpoena to Produce Documents, Information, or Objects or to Permit Inspection of Premises in a Civil Action
http://www.uscourts.gov/uscourts/FormsAndFees/Forms/AO088B.pdf

Sample National Security Letters
http://vault.fbi.gov/National%20Security%20Letters%20%28NSL%29/National%20Security%20Letters%20%28N

SL%29%20Part%201%20of%201

http://www.ala.org/offices/sites/ala.org.offices/files/content/oif/ifissues/nationalsecurityletter.pdf

U.S. Foreign Intelligence Surveillance Court

Public Filings
http://www.uscourts.gov/uscourts/courts/fisc/index.html

Phone Records Order http://www.scribd.com/doc/168957202/FISA-Court-phone-records-order

Sample FISA (section 215) Order for Business Records

U.S. Congress. House Judiciary Subcommittee on Crime, Terrorism and Homeland Security
"FISA provisions authorizing Roving Surveillance, Lone Wolf and Business Records"
Statement of Todd Hinnen, Acting Assistant Attorney General for National Security (March 9, 2011)
http://www.justice.gov/nsd/opa/pr/testimony/2011/nsd-testimony-110309.html

Note: FISA has approved the Department of Justice's request to modify the telephony metadata program
U.S Office of the Director of National Intelligence. Official Statement, Feb. 6, 2014
http://icontherecord.tumblr.com/post/75842023946/fisc-approves-governments-request-to-modify

Also check the laws and regulations governing court orders in your state courts

Statements of Other Library and Professional Associations

ACM Privacy Policy (Association for Computing Machinery) http://www.acm.org/about/privacy-policy

Canadian Library Association Position Statement on Access to Information and Communication Technology (ICT) *Approved by Executive Council – 18 June 1994; amended – 29 May 2012 and affirmed at CLA AGM – 1 June 2012*
http://www.cla.ca/AM/Template.cfm?Section=Position_Statements&Template=/CM/ContentDisplay.cfm&ContentID=3046

IFLA, "The Glasgow Declaration on Libraries, Information Services and Intellectual Freedom. 19 August 2002
http://www.ifla.org/publications/the-glasgow-declaration-on-libraries-information-services-and-intellectual-freedom

IFLA, "The IFLA Internet Manifesto" http://www.ifla.org/files/assets/faife/publications/policy-documents/internet-manifesto-en.pdf (The Hague, Netherlands: IFLA, August 23, 2002).

Other Codes of Ethics for Computing and Information Sciences http://www.emr.org/linksUCE.html

Federal Privacy Laws, Policies and Programs

Privacy Act of 1974; http://www.justice.gov/opcl/privstat.htm

U.S. Dept. of Justice, Office of Privacy and Civil Liberties. *Overview of the Privacy Act of 1974*, 2012 http://www.justice.gov/opcl/1974privacyact-2012.pdf

This act, 5 U.S.C. § 552a (2006), can generally be characterized as an omnibus "code of fair information practices" that attempts to regulate the collection, maintenance, use, and dissemination of personal information by federal executive branch agencies. However, the Act's imprecise language, limited legislative history, and somewhat outdated regulatory guidelines have rendered it a difficult statute to decipher and apply. Moreover, even after more than thirty-five years of administrative and judicial analysis, numerous Privacy Act issues remain unresolved or unexplored. Adding to these interpretational difficulties is the fact that many earlier Privacy Act cases are unpublished district court decisions. A particular effort is made in this "Overview" to clarify the existing state of Privacy Act law while at the same time highlighting those controversial, unsettled areas where further litigation and case law development can be expected.

History of the Privacy Act http://www.cavebear.com/archive/nsf-dns/pa_history.htm

Cable Communications Policy Act of 1984 http://www.law.cornell.edu/uscode/text/47/551

This act, 47 U.S. Code §551, restricts access to cable television subscriber information.

Children's Online Privacy Protection Act (COPPA) http://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

COPA, 15 U.S.C. § 6501; 16 CFR 312, requires commercial online content providers who either have actual knowledge that they are dealing with a child 12 or under or who aim their content at children to obtain verifiable parental consent before they can collect, archive, use, or resell any personal information pertaining to that child. In addition, the Act requires commercial Web sites and online services covered by COPPA to place their information collection, use and disclosure practices prominently on their Web site. The law also mandates that site operators allow parents to review and delete information about their children collected by the site.

Communications Assistance to Law Enforcement Act (CALEA) of 1994
http://www.law.cornell.edu/uscode/text/18/2522
http://www.fcc.gov/encyclopedia/communications-assistance-law-enforcement-act

CALEA, 18 USC §2522, requires a "telecommunications carrier," as defined by the Act, to ensure that equipment, facilities, or services that allow a customer or subscriber to "originate, terminate, or direct communications," enable law enforcement officials to conduct electronic surveillance pursuant to court order or other lawful authorization.

Legal Challenge

American Council on Education v. Federal Communications Commission and United States of America, 451 F.3d 226 (D.C. Cir. 2006) http://law.justia.com/cases/federal/appellate-courts/F3/451/226/627290/

Library Amicus Brief in Support of Plaintiffs. http://www.arl.org/focus-areas/court-cases/2057-american-council-on-education-et-al-v-federal-communications-commission-amicus-brief-in-support-of-ace

Critical Infrastructure Information Protection

http://www.dhs.gov/protected-critical-infrastructure-information-pcii-program

This Program is an information-protection program that enhances voluntary information sharing between infrastructure owners and operators and the government. PCII protections mean that homeland security partners can be confident that sharing their information with the government will not expose sensitive or proprietary data.

Digital Millennium Copyright Act of 1998
http://www.copyright.gov/title17/92chap5.html#512

Section 512 contains a provision to ensure that service providers are not placed in the position of choosing between limitations on liability on the one hand and preserving the privacy of their subscribers, on the other. Subsection (m) explicitly states that nothing in section 512 requires a service provider to monitor its service or access material in violation of law (such as the Electronic Communications Privacy Act) in order to be eligible for any of the liability limitations

Do-Not-Call Implementation Act of 2003
http://www.law.cornell.edu/uscode/text/15/6151?qt-us_code_tabs=0#qt-us_code_tabs
http://www.fcc.gov/encyclopedia/do-not-call-list

Pursuant to its authority under the Telephone Consumer Protection Act (TCPA), 47 US Code §227, the FCC established, together with the Federal Trade Commission (FTC), a national Do-Not-Call Registry. The registry is nationwide in scope, applies to all telemarketers (with the exception of certain non-profit organizations), and covers both interstate and intrastate telemarketing calls. Commercial telemarketers are not allowed to call you if your number is on the registry, subject to certain exceptions. As a result, consumers can, if they choose, reduce the number of unwanted phone calls to their homes. The Do-Not-Call Implementation Act, 15 U.S.Code 87A §6151, authorized the Federal Trade Commission to implement and enforce the national do-not-call registry

Driver License Privacy Act [Prohibition on release and use of certain personal information from State motor vehicle records]

This act, 18 U.S. Code §2721, prohibits the release and use of certain personal information from State motor vehicle records.
http://www.law.cornell.edu/uscode/text/18/2721?qt-us_code_tabs=1#qt-us_code_tabs

In *Maracich v. Spears* http://www.supremecourt.gov/opinions/12pdf/12-25_4314.pdf
the Supreme Court ruled that solicitation is not a permissible use of state motor vehicle records under the Driver's Privacy Protection Act.

E-Government Act of 2002
http://www.law.cornell.edu/uscode/text/44/chapter-36

This act, U.S. Code § 3601-3606, requires Federal Agencies to conduct privacy impact assessments.
Office of Management and Budget. OMB Guidance for Implementing the Privacy
Provisions of the E-Government Act of 2002. M-03-22 Sept. 26, 3003
http://www.whitehouse.gov/omb/memoranda_m03-22

Electronic Communications Privacy Act of 1986 (ECPA),
https://it.ojp.gov/default.aspx?area=privacy&page=1285
http://www.law.cornell.edu/uscode/text/18/part-I/chapter-119

History and Analysis: https://www.cdt.org/issue/wiretap-ecpa

ECPA, Public Law 99-508; 18 U.S.Code § 2510-22, includes provisions for access, use, disclosure, interception and privacy protections of electronic communications. The law, which covers various forms of wire and electronic communications, prohibits unlawful access and certain disclosures of communication contents and prevents government entities from requiring disclosure of electronic communications from a provider without proper procedure. ECPA was amended by Sections 209- 212 and 216 of the USA PATRIOT ACT.

The Enhanced Border Security and Visa Entry Reform Act of 2002
http://www.gpo.gov/fdsys/pkg/PLAW-107publ173/pdf/PLAW-107publ173.pdf
Section 201 http://www.law.cornell.edu/uscode/text/8/1721
restricts the use of the information in the system so as to protect privacy, and it creates criminal penalties for the misuse of the information.

The Fair Credit Reporting Act (1970)
http://www.law.cornell.edu/uscode/text/15/chapter-41/subchapter-III
FCRA, 15 U.S. Code §1681, promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies.
Summary of Rights Under FCRA http://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf

Family Educational Rights and Privacy Act (FERPA)
http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html
FERPA, 20 U.S.Code §1232g; 34 CFR Part 99, protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. The main focus of FERPA is to define who can access student records. FERPA grants parents the rights until the child turns 18 years old or attends a school beyond the high school level. The Act spells out the conditions that allow schools to release records without consent to certain designated parties. Title V, section 507 of the USA PATRIOT Act amended FERPA by creating a new exception to the privacy protections.

Federal Trade Commission's Consumer Protection, Privacy Oversight
http://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/our-divisions/division-privacy-and-identity
The Federal Trade Commission Consumer Protection Division, under Section 5 of the FTC Act, administers a privacy program in order to make sure that companies keep the promises they make to consumers about privacy and take precautions to secure consumers' personal information. The Commission has brought a number of cases to enforce the promises in privacy statements, including promises about the security of consumers' personal information.

The Financial Modernization Act of 1999, Title V, Subtitle A (Gramm-Leach-Bliley Act)
http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf
http://www.fdic.gov/regulations/compliance/manual/pdf/VIII-1.1.pdf
This act, 12 U.S. Code §1811, also known as the "Gramm-Leach-Bliley Act" or GLB Act, includes provisions to protect consumers' personal financial information held by financial institutions. There are three principal parts to the privacy requirements: the Financial Privacy Rule, Safeguards Rule and pretexting provisions. The Safeguards Rule requires all financial institutions to design, implement and maintain safeguards to protect customer information. The Rule applies not only to financial institutions

that collect information from their own customers, but also to financial institutions -- such as credit reporting agencies -- that receive customer information from other financial institutions.

Foreign Intelligence Surveillance Act (FISA) (1978)

http://www.law.cornell.edu/uscode/text/50/chapter-36

http://www.fas.org/irp/agency/doj/fisa/.html

FISA, 18 U.S. Code §1801, prescribes procedures for requesting judicial authorization for electronic surveillance and physical search of persons engaged in espionage or international terrorism against the United States on behalf of a foreign power.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

http://www.hhs.gov/ocr/privacy/index.html

HIPAA, Public Law 104-191, required the Secretary to issue privacy regulations governing individually identifiable health information. The HIPPA Privacy Rule provides federal protections for individually identifiable health information held by covered entities and their business associates and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of health information needed for patient care and other important purposes. http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf

Homeland Security Act of 2002

http://www.law.cornell.edu/uscode/text/6

6 U.S. Code §101, adopted after the Sept. 11, 2001 terrorist attacks with the intention of improving U.S. domestic security.

Privacy Protection Act of 1980

http://www.law.cornell.edu/uscode/text/42/2000aa?qt-us_code_tabs=0#qt-us_code_tabs

http://epic.org/privacy/ppa/

42 U.S.Code § 2000aa et seq., protects journalists from being required to turn over to law enforcement any work product and documentary materials, including sources, before it is disseminated to the public.

Right to Financial Privacy Act (1978)

http://www.law.cornell.edu/uscode/text/12/chapter-35?qt-us_code_tabs=1%23qt-us_code_tabs%20

12 U.S. Code § 3401 -3422, enacted to provide the financial records of financial institution customers a reasonable amount of privacy from federal government scrutiny.

Student and Exchange Visitors Information System (SEVIS) http://www.ice.gov/sevis/

The Student and Exchange Visitors Information System (SEVIS), administered by the Department of Homeland Security in partnership with the Department of State and the Department of Education, maintains updated information on approximately one million non-immigrant foreign students and exchange visitors during the course of their stay in the United States each year. Schools are now required to report a foreign student's failure to enroll or if students drop out of their programs. Certain requirements imposed by the Family Educational Rights and Privacy Act (FERPA) are waived and conditions for employment specified.

Telecommunications Act of 1996

7 U.S.C. § 222 was enacted as part of the Telecommunications Act of 1996 and is entitled "Privacy of Customer Information." It states generally that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to . . . customers." To effectuate that duty, § 222 places restrictions on the use, disclosure of, and access to certain customer information

Video Privacy Protection Act of 1988

The Video Privacy Protection Act of 1988, 18 U.S.C. § 2710, was passed in reaction to the disclosure of Supreme Court nominee Robert Bork's video rental records in a newspaper. The Act is not often invoked, but stands as one of the strongest protections of consumer privacy against a specific form of data collection. Generally, it prevents disclosure of personally identifiable rental records of "prerecorded video cassette tapes or similar audio visual material.
http://epic.org/privacy/vppa/
http://www.law.cornell.edu/uscode/text/18/2710

State Privacy Laws Regarding Library Records

http://www.ala.org/offices/oif/ifgroups/stateifcchairs/stateifcinaction/stateprivacy

For current information on privacy-related legislation, see:

EPIC Bill Track: Tracking Privacy, Speech, and Cyber-Liberties Bills
http://epic.org/privacy/bill_track.html

Appendix B: Privacy Bibliography

Books

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, CT: Libraries Unlimited, 2005.

Includes information about the laws affecting personal privacy and privacy in library as well as the impact on accessibility of online information in these settings.

Allen, Anita. *Unpopular Privacy: What Must We Hide?* (Studies in Feminist Philosophy). N.Y.: Oxford University Press, 2011.

A discussion of when government should mandate privacy and when privacy should be a matter of personal choice.

Andrews, Lori. *I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy*. Florence, MA: Free Press, 2012.

Andrews gives concrete examples of misuse of personal information gleaned from the internet, and provides the information we need to protect ourselves from these abuses, including how to remove personal date from aggregator site.

Bennett, Colin. *The Privacy Advocates*: *Resisting the Spread of Surveillance*. Cambridge, MA: MIT Press, 2008.

> Bennett analyzes the people and groups around the world who have risen to challenge the most intrusive surveillance practices by both government and corporations.

Boghosian, Heidi. *Spying on Democracy: Government Surveillance, Corporate Power, and Public Resistance.* San Francisco, CA: City Lights Publishing, 2013

> Boghosian provides the answer to the question 'If you're not doing anything wrong, why should you care if someone's watching you?' She discusses how technology is being used to categorize and monitor people based on their associations, their movements, their purchases, and their perceived political beliefs.

Brin, David. *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* Jackson, TN: Perseus Press, 1998.

Cassel, Elaine. (2004). *The war on civil liberties: How Bush and Ashcroft have dismantled the Bill of Rights.* Chicago, IL: Lawrence Hill Books, 2004.

> Cassell provides a series of examples based on national and international media coverage illustrating the extent to which our individual rights have been curtailed.

Cate, Fred H. *Privacy in the Information Age.* Washington D.C.: Brookings, 1997.

> Includes four sets of principles for protecting information privacy that recognize the significance of individual and collective nongovernmental action, the limited role for privacy laws and government enforcement of those laws, and the ultimate goal of establishing multinational principles for protecting information privacy

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

> Chmara has represented ALA, the Freedom to Read Foundation and the American Booksellers Association on free speech issues. This is a collection of frequently asked questions based on her experiences.

Etzioni, Amitai. *How patriotic is the Patriot Act? Freedom versus security in the age of terrorism.* NY: Routledge, 2004.

Fisher, Louis. *The Constitution and 9/11: Recurring threats to America's freedoms.* Lawrence, KS: University Press of Kansas, 2008.

Foerstel, Herbert N. *Refuge of a Scoundrel; The Patriot Act in Libraries*. Westport, CT: Libraries Unlimited, 2004.

> History of the origins of library surveillance and the implications of the Patriot Act for libraries and booksellers

… *Surveillance in the Stacks, The FBI's Library Awareness Programs*. Westport, CT: Greenwood Publishing, 1999.

> Relying on previously classified FBI reports, Foerstel traces the history of federal library surveillance, documents the media and congressional response to the Library Awareness Program, and discusses the professional and legislative moves that were taken to safeguard library confidentiality.

Herman, Susan N. *Taking Liberty: The War on Terror and the Erosion of American Democracy* N.Y.: Oxford University Press, 2011.

Includes several chapters on the impact on libraries and librarians.

Lane, Frederick S. *American Privacy: the 400-Year History of Our Most Contested Right*. Boston, MA: Beacon Press, 2009.

A sweeping story of the right to privacy from colonial postal routes to today's fiber-optic cables on a collision course with programmers, librarians and letter-writers.

Levmore, Saul and Martha Nussbaum, eds,, *The Offensive Internet: Speech, Privacy, and Reputation.* Cambridge, MA: Harvard University Press, 2001.

A Collection of essays about the clash between free speech and privacy online.

Magi, Trina J. *Protecting our precious liberties: What every educator needs to know about libraries, privacy and freedom of inquiry.* Bloomington, IN: Phi Delta Kappa International, 2005.

Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life,* Standford, CA*:* Stanford University, 2010.

Nissenbaum persuasively argues that privacy must be understood in its social context, and she provides an insightful and illuminating account of how to do so. For anyone considering the burgeoning problems of information privacy, Privacy in Context is essential reading." —Daniel J. Solove, George Washington University Law School and author of Understanding Privacy

O'Harrow, Robert, Jr. *No Place to Hide.* NY: Free Press, 2002.

O'Harrow, an award-winning Washington Post reporter, describes the emergence of a data-driven surveillance society intent on giving individuals the conveniences and services they crave, like cell phones, discount cards, and electronic toll passes, while watching them more closely than ever before. He shows that since the September 11, 2001, terror attacks, the information industry giants have been enlisted as private intelligence services for homeland security; revealing how people can lose control of their privacy and identities at any moment.

Raul, Alan Charles. *Privacy and the Digital State: Balancing Public Information and Personal Privacy*. Norwell, MA: Kluwer, 2002. http://getebook.org/?p=268106

Raul argues that "privacy" is inherently relative, and is always balanced alongside of various social exigencies, such as other compelling rights guaranteed by the Constitution, the interest of the public in broad disclosure of and access to government records, and the desire to foster an efficient, productive economy. He examines the recurring conflict between "open government" and "privacy of personal information" and attempts to provide a perspective on striking a balance.

Rosen, Jeffrey. The Unwanted Gaze: The Destruction of Privacy in America. N.Y.: Random House, 2000.

Rosen argues that privacy helps to protect us from being judged ''out of context'' -- that is, from having an isolated bit of personal information exposed to the world, so that it becomes our defining characteristic in other people's eyes. Privacy, moreover, helps us to develop close personal relationships and to be creative without fear that our confidential disclosures will be held against us. He suggests that ''privacy is a form of opacity, and opacity has its values. We need more shades and more blinds and more virtual curtains.''

Solove, Daniel J. *The Digital Person: Technology and Privacy in the Information Age*. New York: New York University Press, 2004. http://docs.law.gwu.edu/facweb/dsolove/Digital-Person/text.htm

… The Future of Reputation: Gossip, Rumor, and Privacy on the Internet, New Haven, CT: Yale University Press, 2007.

…. *Nothing to Hide: The False Tradeoff between Privacy and Security*. New Haven, CT: Yale University Press, 2011

…. *Privacy Law Fundamentals*, International Association of Privacy Professionals. (IAPP). 2d Ed., Portsmouth, NH, 2013

…. *Understanding Privacy*. Harvard University Press, 2008.
A comprehensive, conceptual and clear analysis of privacy.

Articles and Reports

American Library Association. Office for Intellectual Freedom, Jason Griffey, Sarah Houghton-Jan, and Eli Neiburger. "Privacy and Freedom of Information in 21st-Century Libraries". *Library Technology Reports*, 46, no. 8 (November/December 2010)

…. Task Force on Privacy and Confidentiality in the Electronic Environment. "Final Report*"* July 7, 2000. http://www.ala.org/lita/about/taskforces/dissolved/privacys

Armen, Keteyian, "Digital Photocopiers Loaded With Secrets" CBS April 2010. http://www.cbsnews.com/news/digital-photocopiers-loaded-with-secrets/

Bernstein, Joen E. "Train Employees and Officials to Be Ready for Privacy Challenges."
Computers in Libraries 27, no. (June 6, 2007): 6 – 9.
http://www.infotoday.com/cilmag/jun07/Bernstein.shtml

Brandt, Allen. *On Making Privacy Policies More Simple and User-Friendly,*
(December 10, 2013)
https://www.privacyassociation.org/privacy_perspectives/post/on_making_privacy_policies_more_simple_and_user_friendly

California Digital Library, SOPAG Privacy Audit and Guidelines
http://libraries.universityofcalifornia.edu/groups/files/sopag/privacy/privacy_audit_guidelines_13aug2001.pdf

Chmara, Theresa. "Minors' Rights to Receive Information Under the First Amendment" (Februry 2, 2004).
http://www.ala.org/Template.cfm?Section=issuesrelatedlinks&Template=/ContentManagement/ContentDisplay.cfm&ContentID=28210

Coyle, Karen. "Make Sure You Are Privacy Literate." *Library Journal* 127, no. 16 (October 1, 2002): 55 - 57. (Preprint available at http://www.kcoyle.net/privacy_lj2.html).

Doyle, Charles. *Libraries and the USA PATRIOT Act: CRS Report to Congress.* Washington, DC: Library of Congress, 2005. http://www.fas.org/sgp/crs/intel/RS21441.pdf

David H. Flaherty, David H. "How to Do a Privacy and Freedom of Information Act Site Visit." (2001) http://www.pco.org.hk/english/infocentre/files/flaherty-2.doc

Fordham Law School. Center on Law and Information Policy. *Curriculum for privacy education geared to middle school students.* http://law.fordham.edu/assets/CLIP/2013_CLIP_VPE_Complete.pdf

Slides
http://law.fordham.edu/assets/CLIP/2013_CLIP_VPE_Passwords_BehavioralAds(1).pptx
http://law.fordham.edu/assets/CLIP/2013_CLIP_VPE_SocialNetworking.pptx
http://law.fordham.edu/assets/CLIP/2013_CLIP_VPE_CellPhones_WiFi_FacialRecog.pptx
http://law.fordham.edu/assets/CLIP/2013_CLIP_VPE_Reputation.pptx

Gellman, Robert. *Fair Information Practices: A Basic History.* Version 1.89, April 25, 2012 http://bobgellman.com/rg-docs/rg-FIPShistory.pdf

Greenleaf, Graham, (2013). "Sherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories", *Journal of Law, Information & Science, (*2013) *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2280877*

The Global Tables of Data Privacy Laws and Bills (3rd Ed, June 2013) analyzed in this article are at http://ssrn.com/abstract=228

Holley, Robert P., "Are Libraries Compromising Reader Privacy with Circulation Reminders?" *Indiana Libraries* 32, no. 1 (2013): 37 – 41 http://journals.iupui.edu/index.php/IndianaLibraries/issue/view/211

Jaeger, Paul T., John Carlo Bertot, Charles R. McClure. "The Impact of the USA Patriot Act on Collection and Analysis of Personal Information under the Foreign Intelligence Surveillance Act." *Government Information Quarterly,* 20, no. 3 (July 2003): 295-314.

Johnston, Scott D. "Rethinking Privacy in the Public Library" *International Information & Library Review* 32, no. 3-4 (September 2000): 509 – 517.

Kleve, Pieter and Richard V. De Mulder. "Privacy Protection and the Right to Information: In Search of a New Symbiosis in the Information Age." Cyberlaw, Security & Privacy (2007): 201-212. *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1138287*

"The dichotomy between personal privacy and free access to information, which has come increasingly to the fore with the advance of information technology, justifies a reconsideration of these traditional values and interests. In this article, it is contended that privacy, as a constitutional right, is subject to changing norms as a result of the advent of the information society. In today's information society, citizens weigh the importance of protecting privacy against the advantages of free access to information. The criterion they use is a rational one: an evaluation of which option provides the individual with the most benefit. The protection of privacy is no longer an unconditional good. For state organisations to champion privacy at any cost is, therefore, out of step with this development. A new balance has to be established between the citizen's right to privacy and their right to know, taking into account this shift in values. In order to prevent on the one hand overzealous protection and, on the other, the abuse of information, it is necessary to set up the monitoring function in a new way."

Klinefelter. Anne, "Library Standards for Privacy: A Model for the Digital World?" *North Carolina Journal of Law & Technology 11,* no 3; Special *(*2010): 553*.* http://jolt.unc.edu/sites/default/files/Gibbons_Llewellyn_v11i3_531_552.pdf

Kranich, Nancy. (2004). "Another Hysteric Librarian for Freedom," In *Censored: 2005, edited by* Peter Phillips and Project Censored, 9-13. New York: Seven Stories Press, 2004.

…. "The Impact of the USA PATRIOT Act on Free Expression," New York: Free Expression Policy Project, (May 2003) http://www.fepproject.org/commentaries/patriotact.html; "Update," (August 27, 2003) http://www.fepproject.org/commentaries/patriotactupdate.html

…. "Librarians and Teen Privacy in the Age of Social Networking," *Knowledge Quest,* 6, no 2, (November/December 2007): 34-37. Available from EBSCO

Lamdan, Sarah Shik. "Why Library Cards Offer More Privacy Rights than Proof of Citizenship: Librarian Ethics and Freedom of Information Act Requestor Policies." *Government Information Quarterly* 30, no. 2 (April 2013): 131-140*.*

This paper demonstrates the divergent requestor privacy policies of professional librarians and the administration of the Freedom of Information Act (FOIA), and urges the federal government to adhere to librarian ethics in order to protect FOIA requestors.

Levinson-Waldman, Rachel. "What the Government Does with American's Data". NY: Brennan Center, 2013 http://www.brennancenter.org/sites/default/files/publications/What%20Govt%20Does%20with%20Data%20100813.pdf

Our lives are composed of small details. Any one detail, standing alone, may provide little insight into one's identity, but the aggregation of details can paint a surprisingly accurate and revealing picture.

Magi, Trina J. "A Content Analysis of Library Vendor Privacy Policies: Do They Meet Our Standards? *College and Research Libraries* 71, no.3 (May 2010): 254 – 272. http://crl.acrl.org/content/71/3/254.full.pdf

…. "Fourteen Reasons Privacy Matters: A Multidisciplinary Review of Scholarly Literature," *The Library Quarterly* 81, no. 2 (April 2011): 187-209. (Available from JSOR)

This article attempts to expand librarians' understanding by reviewing scholarly literature on privacy from a wide variety of disciplines outside the field of library science, including anthropology, law, philosophy, political science, psychology, and sociologyAfter discussing the challenges of defining privacy and addressing the question of whether privacy is a value that spans cultures, the article traces a number of major themes in the literature, enumerating a host of individual, interpersonal, and societal goods that are made possible by privacy.

… "A Fresh Look at Privacy-Why Does It Matter, Who Cares, and What Should Librarians Do about It?" *Indiana Libraries,* Vol. 32, no. 1 (2013): 34 – 36 http://journals.iupui.edu/index.php/IndianaLibraries/issue/view/211

Meyer, David. "Without the Option of Privacy We Are Lost." (July 10, 2013).

http://gigaom.com/2013/07/10/without-the-option-of-privacy-we-are-lost/

Minow, Mary. “The USA PATRIOT Act and Patron Privacy on Library Internet Terminals” *Library and Technology Resources for Legal Professionals (*February 15, 2002). http://www.llrx.com/features/usapatriotact.htm

Molz, R. Kathleen, “Intellectual Freedom and Privacy: Comments on a National Program for Library and Information Services.” National Commission on Libraries and Information Science. National Program for Library and Information Services. Related Paper Number 10, December, 1974. ED 100 395. http://files.eric.ed.gov/fulltext/ED100395.pdf

The civil libertarian aspects of the National Program for Library and Information Science, including the right of privacy, are analyzed. Includes a chronology of events relating to intellectual freedom and privacy from 1950 – 1974.

OCLC. “Sharing, Privacy and Trust in Our Networked World: a Report to the OCLC Membership”. 2007 http://www.oclc.org/reports/sharing.en.html

Organization for Economic and Cultural Development (OECD). “Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data” (July 11, 2013) http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

O’Neill, Ben. “Edward Snowden, the NSA, and the US Courts.” Ludwig von Mises Institute, February 12, 2014. http://mises.org/daily/6662/Edward-Snowden-the-NSA-and-the-US-Courts

…. “FISA, the NSA, and America's Secret Court System” *Right Side News,* February 24, 2014. http://www.rightsidenews.com/2014022433911/us/homeland-security/fisa-the-nsa-and-america-s-secret-court-system.html

Oregon State Public Interest Research Group. “Resource Guide to Online Privacy; How to Keep Your Personal Information Safe Online” Last updated 11/7/2013 http://ospirg.org/onlineprivacy

Pew Research Center. Internet & American Life Project. “Anonymity, Privacy and Security Online.” (September 5, 2013). http://pewinternet.org/Reports/2013/Anonymity-online.aspx

A report based on telephone interviews conducted by Princeton Survey Research Associates International from July 11-14, among a sample of 1,002 adults ages 18 and older.

Privacy International. “The State of Privacy 2014.” https://www.privacyinternational.org/blog/the-state-of-privacy-2014

Privacy International is a registered UK charity and the first organization to campaign at an international level on privacy issues. They publish a report on the state of privacy in the world each year.

Privacy Rights Clearinghouse. “Privacy Survival Guide; Take Control of Your Personal Information. (Revised March 2014) https://www.privacyrights.org/privacy-survival-guide-take-control-your-personal-information

Reidenberg, Joel R.; N. Cameron Russell; Jordan Kovnot; Thomas B. Norton; Ryan Cloutier, and Daniela. "Privacy and Cloud Computing in Public Schools". (2013). *Center on Law and Information Policy.* Book 2.

http://ir.lawnet.fordham.edu/clip/2

Rubel, Alan. (2007). "Privacy and the USA Patriot Act: Rights, the Value of Rights, and Autonomy," *Law and Philosophy* 26, n2, (March 2007): 119-159. *papers.ssrn.com/sol3/papers.cfm?abstract_id=881130*

Sales, Nathan. "Mending Walls: Information Sharing After the USA PATRIOT Act," *Texas Law Review*. 88, no.7 (June 2010) : 1795-1854. Available from Academic Search Premier.

This Article attempts to fill that gap in the literature. It has three goals: to weigh the advantages and disadvantages of information sharing; to identify some of the remaining legal restrictions on data exchange, as well as their policy justifications; and to consider whether these laws' underlying values can coexist with expanded sharing.

Schwartz, Paul M. and Daniel J. Solove. "The PII Problem: Privacy and a New Concept of Personally Identifiable Information". *New York University Law Review,* 86, no.6, (December 2011): 1815 – 1894. http://ssrn.com/abstract=1909366

Schneier, Bruce. "The Eternal Value of Privacy." *Wired,* May 18, 2006
http://www.wired.com/politics/security/commentary/securitymatters/2006/05/70886

Solove. Daniel J. "The Future of Privacy," *American Libraries* 39, no. 8, (September 2008): 56-59. Available from Ebscohost

Solove argues that Privacy helps to protect us from being judged ''out of context'' -- that is, from having an isolated bit of personal information exposed to the world, so that it becomes our defining characteristic in other people's eyes. Privacy, moreover, helps us to develop close personal relationships and to be creative without fear that our confidential disclosures will be held against us. In a culture of transparency and fleeting attention spans, Rosen observes, ''privacy is a form of opacity, and opacity has its values. We need more shades and more blinds and more virtual curtains."

…. "I've Got Nothing to Hide' and Other Misunderstandings of Privacy." *San Diego Law Review*, Vol. 44 no. 4 (Fall 2007): 745-772. Available from LexisNexis Academic

Starr, Joan. "Libraries and National Security: An Historical Review." *First Monday* 9, no. 12 (December 2004) http://journals.uic.edu/ojs/index.php/fm/article/view/1198/1118

Strickland, L.S., & Hunt, L.E. (2005) "Technology, Security, and Individual Privacy: New Tools, New Threats, and New Public Perceptions." *Journal of the American Society for Information Science & Technology*, 56, no.3. (February 2005): 221-234.

Radio frequency identification (RFID) tags and smart cards are becoming ubiquitous in government and business. Directly or indirectly, in many of these applications, individuals and their activities are tracked. Based on a survey of individuals the authors conclude that a primary objective for any organization using these technologies should be to develop a comprehensive Technology Privacy Policy. The article includes detailed specifications for such a policy.

Texas Department of Information Resources, "Privacy Issues Involved in Electronic Government." http://tinyurl.com/mv8rym5 (2000)

Thierer, Adam. (2011). "Kids, Privacy, Free Speech & the Internet: Finding the Right Balance." Working

Paper, Mercatus Center, George Mason University, http://mercatus.org/publication/kids-privacy-free-speech-internet

U.S. Department of Commerce. *Commercial Data Privacy and Innovation in the Internet Economy*. *Internet Policy Task Force Green Paper* (December 16, 2010)
http://www.ntia.doc.gov/report/2010/commercial-data-privacy-and-innovation-internet-economy-dynamic-policy-framework
"America needs a robust privacy framework that preserves consumer trust in the evolving Internet economy while ensuring the Web remains a platform for innovation, jobs, and economic growth. Self-regulation without stronger enforcement is not enough. Consumers must trust the Internet in order for businesses to succeed online." said Commerce Secretary Gary Locke. "Today's report is a road map for considering a new framework that is good for consumers and businesses. And while our primary goal is to update the domestic approach to online privacy, we are optimistic that we can take steps to bridge the different privacy approaches among countries, which can help us increase the export of U.S. services and strengthen the American economy."

U.S. Department of Education. Family Policy Compliance Office Web Site
http://www2.ed.gov/policy/gen/guid/fpco/index.html

U.S. Department of Education. Privacy Technical Assistance Center
Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices.
Center:
http://ptac.ed.gov/sites/default/files/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29.pdf
This document addresses privacy and security considerations relating to computer software, mobile applications (apps), and web-based tools provided by a third-party to a school or district that students and/or their parents access via the Internet and use as part of a school activity. Examples include online services that students use to access class readings, to view their learning progression, to watch video demonstrations, to comment on class activities, or to complete their homework.

U.S. Department of Education. Secretary's Advisory Committee on Automated Personal Data Systems. "Records, Computers and the Rights of Citizens" (July 19973). Includes "Fair Information Practice Principles." http://epic.org/privacy/hew1973report/

U.S. Federal Trade Commission, "FTC Strengthens Kid's Privacy, Gives Parents Greater Control Over Their Information By Amending Children's Online Protection Rule." December 19, 2012.
http://www.ftc.gov/opa/2012/12/coppa.shtm

…. "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policy Makers." (March 2012)
http://www.ftc.gov/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations

U.S. Federal Trade Commission. Bureau of Consumer Protection. Business Center. "Complying with COPPA: Frequently Asked Questions : A Guide for Business and Parents and Small Entity Compliance Guide." (July 2013).
http://www.business.ftc.gov/documents/0493-Complying-with-COPPA-Frequently-Asked-Questions

These FAQs "are intended to supplement the compliance materials available on the FTC website. In addition, you may send questions or comments to the FTC staff's COPPA mailbox, CoppaHotLine@ftc.gov**.** This document represents the views of FTC staff and is not binding on the Commission. To view the Rule and compliance materials, go to the FTC's COPPA page for businesses**.** This document serves as a small entity compliance guide pursuant to the Small Business Regulatory Enforcement Fairness Act.

Some FAQs refer to a type of document called a Statement of Basis and Purpose. A Statement of Basis and Purpose is a document an agency issues when it promulgates or amends a rule, explaining the rule's provisions and addressing comments received in the rulemaking process. A Statement of Basis and Purpose was issued when the COPPA Rule was proposed.

…."Children's Privacy. http://www.business.ftc.gov/privacy-and-security/childrens-privacy

U.S. National Institute of Standards and Technology. Information Security and Privacy Advisory Board. "Toward A 21st Century Framework for Federal Government Privacy Policy" (May 2009). http://csrc.nist.gov/groups/SMA/ispab/documents/correspondence/ispab-report-may2009.pdf

Analyses issues and makes recommendations for updating privacy law and policy in light of technological change.

U.S. White House. *Consumer Data Privacy in a Networked World: A Framework of Protecting Privacy and Promoting Innovation in the Global Digital Economy.* (February, 2012) http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

Warren, Samuel & Brandeis, Louis. "The Right to Privacy." Harvard Law Review 4, no.5 (December 1890): 193-220. http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

Source of "the right to be let alone," this foundational document has been called one of the most influential essays in the history of American law. Reflecting the upper class concerns of its day, it addresses commercial exploitation of gossip and technological aids to an invasive press, rather than Big Brother government surveillance.

Wheeler, Maurice. "The Politics of Access: Libraries and the Fight for Civil Liberties in Post-9/11 America," *Radical History Review*, 93, (Fall 2005): 79-95.

Wolf, Christopher and Jules. "An Updated Privacy Paradigm for the "Internet of Things"' November 19, 2013 http://www.futureofprivacy.org/wp-content/uploads/Wolf-and-Polonetsky-An-Updated-Privacy-Paradigm-for-the-%E2%80%9CInternet-of-Things%E2%80%9D-11-19-2013.pdf

Zimmer, Michael. "Assessing the Treatment of Patron Privacy in Library 2.0 Literature". *Information Technology and Libraries*, 32, no. 2 (June 2013): 29–41.

An ethical examination of the emergence of new Library 2.0 tools and technologies in relation to existing ethical norms of information flow within the library context. Available from Ebscohost.

…. "Librarian attitudes regarding information and Internet privacy". Library Quarterly, 84, no.2 (April 2014):123-151. Available from JSTOR and Chicago Journals.

A report of findings from a new survey measuring librarians' views on privacy rights and protecting library users' privacy. The study, which builds on a 2008 ALA survey assessing librarians' attitudes about

privacy, provides important data that will help privacy advocates evaluate the state of privacy in the United States and libraries' role in protecting library users' privacy. Overall, the results indicate a high level of concern among respondents over information privacy and a desire to control access and use of personal information, but they also reflect some shifts in privacy attitudes compared to the 2008 study. Implications are discussed for future advocacy and outreach by the American Library Association and related advocacy and educational groups

…. "Patron Privacy in the '2.0' Era: Avoiding the Faustian Bargain of Library 2.0." *Journal of Information Ethics*, 22, no.1 (Spring 2013): 44–59 Available from Metapress.

An ethical examination of the emergence of new Library 2.0 tools and technologies in relation to existing ethical norms of information flow within the library context.

Privacy Websites

American Civil Liberties Association https://www.aclu.org/time-rein-surveillance-state-0

American Library Association http://www.ala.org/search/site/privacy?f[0]=hash%3Amf0qin

Center for Democracy and Technology https://www.cdt.org/; http://consumerprivacyguide.org/

Choose Privacy Week http://chooseprivacyweek.org/

CNET News: Security & Privacy http://news.cnet.com/security/

Electronic Frontier Foundation https://www.eff.org/issues/privacy

Electronic Privacy Information Center (EPIC) Privacy Blog http://epic.org/blog/

The Future of Privacy Forum www.futureofprivacy.org

International Association of Privacy Professionals https://www.privacyassociation.org/

OECD http://www.oecd.org/general/searchresults/?q=privacy%20guidelines

The Privacy Coalition http://privacycoalition.org/

Privacy.org http://privacy.org/

Privacy Association https://www.privacyassociation.org

Privacy International https://www.privacyinternational.org/

Privacy Rights Clearinghouse https://www.privacyrights.org/

Worlds of David Brin http://www.davidbrin.com/transparency.html