Library Technology
REPORTS
Expert Guides to Library Systems and Services

Library Privacy Policies

Jason Vaughan

ALA TechSource
alatechsource.org
American Library Association

Library Technology
REPORTS

ALA TechSource purchases fund advocacy, awareness, and accreditation programs for library professionals worldwide.

Volume 56, Number 6
Library Privacy Policies
ISBN: 978-0-8389-4677-0
DOI: https://doi.org/10.5860/ltr.56n6

American Library Association
225 N. Michigan Ave., Suite 1300
Chicago, IL 60601-7616 USA
alatechsource.org
800-545-2433, ext. 4299
312-944-6780
312-280-5275 (fax)

Advertising Representative
Patrick Hogan
phogan@ala.org
312-280-3240

Editor
Patrick Hogan
phogan@ala.org
312-280-3240

Copy Editor
Judith Lauber

Production
ALA Production Services

Cover Design
Alejandra Diaz and ALA Production Services

Library Technology Reports (ISSN 0024-2586) is published eight times a year (January, March, April, June, July, September, October, and December) by American Library Association, 225 N. Michigan Ave., Suite 1300, Chicago, IL 60601-7616. It is managed by ALA TechSource, a unit of the publishing department of ALA. Periodical postage paid at Chicago, Illinois, and at additional mailing offices. POSTMASTER: Send address changes to Library Technology Reports, 225 N. Michigan Ave., Suite 1300, Chicago, IL 60601-7616.

About the Author

Jason Vaughan is a full professor and director of library technologies at the University of Nevada, Las Vegas Libraries. As a senior leader at the library, he provides oversight for library systems and web and application development services. He has been co–principal investigator on numerous grants and is the author of two previous issues of *Library Technology Reports*, "Web Scale Discovery Services" and "Technological Innovation: Perceptions and Definitions." He holds an MLS and a BA from the University of North Carolina at Chapel Hill.

Abstract

Protecting patron privacy in an increasingly distributed online environment is a complex challenge facing libraries. Still, publicly posted privacy policies can empower patrons, allow librarians to share their professional values, and help support sound library operations in the event of information disclosure requests. This issue of *Library Technology Reports* (vol. 56, no. 6), "Library Privacy Policies," shares results from an analysis of publicly posted privacy policies from one hundred academic and public libraries across the United States. Details on data types, why data is collected, how data is used and protected, and how data may be released are shared. Just as importantly, nuances in how policy text is phrased reveals a richness and emphasizes the adage that "It's not always what you say, but how you say it."

Subscriptions

alatechsource.org/subscribe

Contents

Contents, continued

Chapter 1

Introduction and Demographics

In an increasingly distributed online environment, libraries find themselves challenged in their efforts to uphold core professional tenets focused on patron privacy. The tension is not new. At a broad level, the US Federal Trade Commission (FTC) has been studying online privacy issues since 1995, releasing several reports to Congress, including *Privacy Online: Fair Information Practices in the Electronic Marketplace*.[1] Even earlier, with origins dating to 1973, before the advent of the modern web, the FTC released its Fair Information Practice Principles, which "included a blend of substantive (e.g., data quality, use limitation) and procedural (e.g., consent, access) principles" that "reflected a wide consensus about the need for broad standards to facilitate both individual privacy and the promise of information flows in an increasingly technology-dependent, global society."[2] In 2015, the National Information Standards Organization (NISO) released its *NISO Consensus Principles on User's Digital Privacy in Library, Publisher, and Software-Provider Systems*. The preamble notes, "The management of information resources increasingly involves digital networks that, by their nature, include possibilities for tracking and monitoring of user behavior. . . . Libraries, publishers, and software-providers have a shared obligation to foster a digital environment that respects library users' privacy as they search, discover, and use those resources and services."[3] Tilting the focus even more specifically toward libraries, the American Library Association (ALA) released its first comprehensive Privacy Tool Kit in 2005. This guidance has subsequently been revised and updated through the efforts of ALA's Office for Intellectual Freedom and the Intellectual Freedom Committee (and associated Privacy Subcommittee). Indeed, ALA has long been a staunch advocate of patron privacy, as evidenced by its extensive research, advocacy work, and published statements, including the following:

- "Policy on Confidentiality of Library Records"[4]
- *Privacy: An Interpretation of the Library Bill of Rights*[5]
- *Resolution on the Retention of Library Usage Records*[6]
- "Policy Concerning Confidentiality of Personally Identifiable Information about Library Users"[7]

The present Privacy Tool Kit's introduction notes,

> The danger of invasion of personal privacy is a very real concern and often challenges existing library state privacy and confidentiality laws. . . . 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.[8]

An oft-quoted foundational passage from *Privacy: An Interpretation of the Library Bill of Rights* notes, "In a library (physical or virtual), the right to privacy is the right to open inquiry without having the subject of one's interest examined or scrutinized by others."[9] ALA's *Resolution on the Retention of Library Usage Records* notes, "The American Library Association urges all libraries to adopt or update a privacy policy protecting users' personally identifiable information, communicating to library users how their information is used, and explaining the limited circumstances under which personally identifiable information could be disclosed."[10] At least part of the substance of many libraries' local privacy policies is modeled on the recommendations found within the Privacy Tool Kit.

On the global stage, in 2002 the International Federation of Library Associations (IFLA) released *The Glasgow Declaration on Libraries, Information Services and Intellectual Freedom*, which includes the statement

"Libraries and information services shall protect each user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted."[11] That same year the organization released the *IFLA Internet Manifesto*, which notes, "Libraries and information services should respect the privacy of their users and recognize that the resources they use should remain confidential."[12] More recently, in 2015, IFLA released a *Statement on Privacy in the Library Environment*. It includes eight recommendations and further notes,

> Library and information services can decide what kind of personal data they will collect on users and consider principles of data security, management, storage, sharing and retention. They can negotiate with commercial service providers to ensure the protection of users' privacy, refuse to acquire services that collect excessive data, or limit the use of technologies that could compromise users' privacy. However, library and information services' opportunities to influence, regulate or gain reliable knowledge of the data collection practices of commercial vendors or government institutions may be limited.[13]

A half century ago, Westin noted that privacy can be defined as "the claim of individuals, groups, or institutions to determine when, how, and to what extent information about them is communicated to others."[14] Malaga, summarizing published research from the late twentieth century as the consumer web began to emerge, noted, "In the context of online transactions privacy involves two major components. The first is the right to be informed about the collection of personal data. The second is a determination over who controls the data and its dissemination."[15]

Privacy also involves security. As Flavian and Guinaliu noted,

> Privacy is linked to a set of legal requirements and good practices with regard to the handling of personal data, such as the need to inform the consumer at the time of accepting the contract what data are going to be collected and how they will be used. Security refers to the technical guarantees that ensure that the legal requirements and good practices with regard to privacy will be effectively met.[16]

Herein we have several cornerstones informing the conversation related to library privacy policy efforts. Regardless of present-day technological and legal complexities, policies still matter. As Vail and colleagues noted, "One way that companies seek to increase trust is by posting a privacy policy notice on their website. . . . To increase consumer trust, it is essential that companies post privacy policies that are both concise and comprehensible."[17] As Earp and colleagues noted, "Internet privacy policies describe an organization's practices on data collection, use, and disclosure. These privacy policies both protect the organization and signal integrity commitment to site visitors. Consumers use the stated website policies to guide browsing and transaction decisions."[18] As Magi noted, "Librarians can make ethical principles operational at the local level by adopting policies that affirm the professional code of ethics. Policies enable an organization to behave in accordance with its mission and philosophy."[19]

Magi further noted several sets of past research whose authors (Nelson and Garcia; Stueart and Moran; Becker)[20] articulated the importance of library policies from both the library staff operational standpoint and the end-user information consumer standpoint, in the sense that library policies can

- reinforce library priorities
- empower library workers
- foster conduct consistency and uniformity
- encourage stability
- reduce confusion
- illustrate accountability
- advise the public on expectations and equitable treatment
- provide guidance should legal action arise[21]

ALA's *Privacy: An Interpretation of the Library Bill of Rights* notes,

> 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.[22]

Leveraging the work of various organization committees, ALA has published extensive Library Privacy Guidelines and associated Library Privacy Checklists.[23] Collectively these resources provide excellent guidance on policy development and content.

Among its wealth of information ALA's Privacy Tool Kit notes,

> 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.[24]

> 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.[25]
>
> All libraries—not just those that are publicly funded—should have in place privacy policies and procedures to ensure that confidential information in all formats is protected. A privacy policy communicates the library's commitment to protecting user information and helps prevent liability and public relations problems.[26]

Purpose of This Report

If privacy policies are important, then how are academic and public libraries faring? This report constitutes a content analysis of privacy policies across a broad swath of academic and public libraries in the United States—fifty selected libraries within each category. The research focuses on several privacy policy aspects: specifically, do the policies

- provide details on what data is collected and what systems are involved?
- provide details on how collected data is used?
- provide details on third-party providers and services utilized by the library?
- provide details on operational data security, integrity, and retention practices?
- reference higher authorities (e.g., organizational statements, parent institution policies, state and federal law)?
- provide details on circumstances in which private information could be released?

In addition, the research surfaces further details that other libraries could consider when drafting a policy for the first time or when updating an existing policy. These include outliers that exist in one or a few policies that other libraries might wish to consider for their own organizations' policies—whether it be a different data type to address or a different policy phrasing to express a particular concept.

The overall intent of this research is multifold. It offers a year 2020 snapshot-in-time assessment of privacy policies from one hundred libraries, offering real-world, in-effect details on what such policies include. In some cases, policies followed a generic template regarding ordering, structure, and topics covered; in many cases, they did not. At another level, this research identifies some not-so-common items found within some of the policies—differences, nuances, and detail outliers when compared to the bulk of the policies analyzed. Some libraries have short and succinct policies, others are more extensive, and many libraries have multiple policies touching on privacy considerations. Finally, and perhaps most significant, while many policies address similar central tenets, a real richness can be found in the variety of verbiage and phrasing found across the policies. For any particular aspect of privacy that a policy seeks to incorporate, there are multiple ways to address that aspect. As a great former boss oft noted, "It's not always what you say, but how you say it." Accordingly, the author has provided numerous examples quoting from the sample set of policies and organized them by topic. It's hoped this approach helps illustrate the myriad ways library privacy policies approach and address particular topics. The quotes are not meant to be taken out of context, but due to manuscript length limitations, snippets (and not necessarily full passages) are provided to address the particular content topic at hand. Readers can always use the references to see the complete policy text of any particular library. In the end, one or more particular policy phrasings quoted in this work may resonate with a particular reader as their own library chooses to draft or revise its privacy policy.

Research Sample and Demographics

For academic libraries, the sample is comprised of major private and public academic libraries based in the United States. The definition of *major* can be subjective. For this research, the author combined and deduplicated library membership lists for academic libraries that were members of all three of the following major organizations—the Association of Research Libraries, the Digital Library Federation, and the Coalition for Networked Information[27]—and subsequently removed libraries not found in the United States. The distilled list of 210 academic libraries was randomized, after which the author proceeded in order down the randomized list, visiting each academic library home page, until fifty libraries were reached that appeared to have their own distinct library privacy policies posted on their library websites. This is an important distinction. In each instance, the larger parent university also appeared to have a (larger, institutional-level) privacy policy, and in many cases the library websites may have provided a link to their parent institutional policy (or referenced it within their own library privacy policy). However, this research intentionally and specifically focuses on library-drafted privacy policies—library policies drafted and linked to the library

website that spoke to something unique, additional, or otherwise seemingly important enough for the library to author and publicly post its own policy—regardless of how long, comprehensive, or unique the specific library policy appeared when compared to any parent institution privacy policy. This is not meant to imply that libraries that appeared not to have their own drafted and posted library privacy policy (and thus were not included in the study sample) do not value or safeguard privacy. Such a fact could mean any number of things, including that the library simply and directly adheres to the parent institution privacy policy and has no interest (or time or authority) to draft its own library policy that may more specifically address some unique aspect, concern, or value of the library. It's also possible that some libraries in the distilled list could have a library-specific privacy policy that simply isn't linked to the library's website, or, if it is linked, the author could simply have failed to find it. However, part of a policy's value lies in being easily found and available to those wishing to review it and who are bound by the policy. For context, the author had to review the websites of the first eighty-five academic libraries in the randomized list until fifty academic libraries appearing to have their own distinct library privacy policies were identified. Privacy policies from these fifty academic libraries were subsequently analyzed for this study. Of the fifty:

- Thirty-three were public institutions, sixteen were private, and one categorizes itself as neither (Penn State University).
- The libraries were spread across twenty-six states from all four regions (West, Midwest, South, Northeast) of the United States.
- Institutional enrollment ranged from 2,000 students (Colby College) to 71,000 students (Rutgers University). The average enrollment for the fifty institutions was 27,940 students, and the median was 27,320 students.

For public libraries, the author leveraged data associated with the Institute of Museum and Library Services' FY 2017 Public Libraries Survey, encompassing data from over 9,200 United States public libraries.[28] The author sorted the libraries by population served, grouping the sets into five size categories: 1–25,000; 25,001–50,000; 50,001–250,000; 250,000–1 million; and > 1 million. The author randomized the libraries within each size group and reviewed the websites of each library until the first ten libraries from each group were identified that appeared to possess their own distinct privacy policies. Given the far greater number of small public libraries in the United States, this approach skews the proportion of overall policies analyzed toward larger service population libraries. While the author analyzed in detail the policies of ten of thirty-four libraries present in the largest service population group, only ten of 7,069 libraries (.14 percent) within the smallest service population group were analyzed. For context, the author had to review the websites of a total of 104 public libraries until fifty were found that appeared to have their own publicly posted and distinct library privacy policy. Regarding the other fifty-four public libraries, in some but not all cases the library website did provide a link to some other privacy policy, such as that for the overarching city or county government entity that library was administratively under. The fifty public libraries analyzed were spread across twenty-five states and all four regions.

Some libraries appeared to have a single unified or encompassing privacy policy, while others incorporated aspects of privacy into multiple policies. For example, one public library—the Alpha Park Public Library—appeared to have eight policies that each in some way touches on privacy:

- "Security/Surveillance System Policy"
- "Reference Policy"
- "Photography and Video Policy"
- "Identity Protection Policy"
- "Ethics Statement for Public Library Trustees"
- "Confidentiality Policy"
- "Computer and Internet Policy"
- "Circulation Policy"[29]

The next chapter details particular data types and systems referenced within library policies. Chapter 3 discusses the stated reasons why data is collected and how it's used, chapter 4 discusses third-party providers and how library policies address such providers, and chapter 5 discusses references to data security, integrity, and retention. The final chapter focuses on references to higher authorities that impact privacy and situations in which private information may be subject to release.

Notes

1. Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace*, report to Congress (Washington, DC: Federal Trade Commission, May 2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.
2. Fred H. Cate, "The Failure of Fair Information Practice Principles," in *Consumer Protection in the Age of the "Information Economy,"* ed. Jane K. Winn (Burlington, VT: Ashgate Publishing, 2006), 343.
3. National Information Standards Organization, *NISO Consensus Principles on User's Digital Privacy in Library, Publisher, and Software-Provider Systems (NISO Privacy Principles)* (Baltimore, MD: National Information

Standards Organization, December 10, 2015), https://groups.niso.org/apps/group_public/download.php/16064/NISO%20Privacy%20Principles.pdf.
4. American Library Association, "Policy on Confidentiality of Library Records," last updated July 2, 1986, www.ala.org/advocacy/intfreedom/statementspols/otherpolicies/policyconfidentiality.
5. American Library Association, *Privacy: An Interpretation of the Library Bill of Rights* (Chicago: American Library Association, 2002, amended 2014, 2019), www.ala.org/advocacy/sites/ala.org.advocacy/files/content/intfreedom/librarybill/interpretations/privacyinterpretation.pdf.
6. American Library Association, *Resolution on the Retention of Library Usage Records* (Chicago: American Library Association, 2006), https://alair.ala.org/bitstream/handle/11213/1594/52.4.4%20Retention%20of%20Library%20Records.pdf.
7. American Library Association, "Policy Concerning Confidentiality of Personally Identifiable Information about Library Users," last updated June 30, 2004, www.ala.org/advocacy/intfreedom/statementspols/otherpolicies/policyconcerning.
8. American Library Association, "Introduction," Privacy Tool Kit, last updated January 2014, www.ala.org/advocacy/privacy/toolkit/introduction.
9. American Library Association, *Privacy*, 1.
10. American Library Association, *Resolution on the Retention*, 2.
11. International Federation of Library Associations, *The Glasgow Declaration on Libraries, Information Services and Intellectual Freedom* (The Hague, Netherlands: International Federation of Library Associations, 2002), https://www.ifla.org/publications/the-glasgow-declaration-on-libraries-information-services-and-intellectual-freedom.
12. International Federation of Library Associations, *IFLA Internet Manifesto* (The Hague, Netherlands: International Federation of Library Associations, 2002), 4, https://www.ifla.org/files/assets/faife/publications/policy-documents/internet-manifesto-en.pdf.
13. International Federation of Library Associations, *IFLA Statement on Privacy in the Library Environment* (The Hague, Netherlands: International Federation of Library Associations, 2015), 2, https://www.ifla.org/files/assets/hq/news/documents/ifla-statement-on-privacy-in-the-library-environment.pdf.
14. Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967), 7.
15. Ross Malaga, "Do Web Privacy Policies Still Matter?" *Academy of Information and Management Sciences Journal* 17, no. 1 (2014): 95.
16. Carlos Flavian and Miquel Guinaliu, "Consumer Trust, Perceived Security and Privacy Policy," *Industrial Management and Data Systems* 106, no. 5 (2006): 604.
17. Matthew Vail, Julia Earp, and Annie Anton, "An Empirical Study of Consumer Perceptions and Comprehension of Web Site Privacy Policies," *IEEE Transactions on Engineering Management* 55, no. 3 (2008): 442.
18. Julia Earp, Annie Anton, Lynda Aiman-Smith, and William Stufflebeam, "Examining Internet Privacy Policies within the Context of User Privacy Values," *IEEE Transactions on Engineering Management* 52, no. 2 (2005): 227.
19. Trina Magi, "The Gap between Theory and Practice: A Study of the Prevalence and Strength of Patron Confidentiality Policies in Public and Academic Libraries," *Library and Information Science Research* 29, no. 4 (2007): 459.
20. Sandra Nelson and June Garcia, "Issues," in *Creating Policies for Results: From Chaos to Clarity* (Chicago: American Library Association, 2003), 1–21; Robert D. Stueart and Barbara Moran, "Planning Information Services," in *Library and Information Center Management*, 6th ed. (Westport, CT: Libraries Unlimited, 2002), 62–90; Beverley Becker, "Essential Preparation," in *Intellectual Freedom Manual*, 7th ed. (Chicago: Office for Intellectual Freedom, American Library Association, 2006), 417–28.
21. Magi, "Gap between Theory and Practice," 459.
22. American Library Association, *Privacy*, 1.
23. American Library Association, "Library Privacy Guidelines," 2017, www.ala.org/advocacy/privacy/guidelines; American Library Association, "Library Privacy Checklists," 2017, www.ala.org/advocacy/privacy/checklists.
24. American Library Association, "Developing or Revising a Library Privacy Policy," Privacy Tool Kit, last updated April 2017, www.ala.org/advocacy/privacy/toolkit/policy.
25. American Library Association, "Developing or Revising."
26. American Library Association, "Privacy and Confidentiality Q&A," last updated July 29, 2019, www.ala.org/advocacy/intfreedom/privacyconfidentialityqa.
27. Association of Research Libraries, "List of ARL Members," https://www.arl.org/list-of-arl-members/; Digital Library Federation, "Our Member Institutions," https://www.diglib.org/about/members/; Coalition for Networked Information, "Members," last updated April 22, 2020, https://www.cni.org/about-cni/membership/members.
28. Institute of Museum and Library Services, "Public Libraries Survey: FY 2017," 2019, https://www.imls.gov/research-evaluation/data-collection/public-libraries-survey.
29. Alpha Park Public Library, "Library Policies and Ordinances," www.alphapark.org/policiesandprocedures.html.

Chapter 2

Systems and Data Referenced

Before listing particular data types and systems referenced in library privacy policies, it's useful to provide a brief and broad perspective. Conversations on patron privacy often leverage three terms or phrases in particular: *privacy* (and *private information*), *confidentiality* (and *confidential information*), and *personally identifiable information*, often abbreviated as *PII*. ALA's *Privacy: An Interpretation of the Library Bill of Rights* can serve as an introduction to the conversation, noting,

> In a library (physical or virtual), the right to privacy is the right to open inquiry without having the subject of one's interest examined or scrutinized by others. Confidentiality exists when a library is in possession of personally identifiable information about users and keeps that information private on their behalf.[1]

The third principle found in ALA's *Code of Ethics* is "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."[2] ALA's Privacy issues and advocacy home page notes,

> The right to privacy—the right to read, consider, and develop ideas and beliefs free from observation or unwanted surveillance by the government or others—is the bedrock foundation for intellectual freedom. It is essential to the exercise of free speech, free thought, and free association.[3]

ALA's "Privacy and Confidentiality Q&A" includes several key questions and answers that help to define the three key terms listed above, including the questions "What is the difference between privacy and confidentiality in a library?" and "What is 'personally identifiable information,' and why is this phrase used?"[4]

The quotes below, drawn directly from some of the analyzed privacy policies in this study, further illuminate these important concepts and begin to provide examples of specific systems, records, data, and transactions associated with library operations that fall under the umbrella of data worthy of protection.

Hutto Public Library

> Records of this library which identify or serve to identify a person who requests, obtains, or uses library materials or services are confidential.[5]

Mount Prospect Public Library

> Patron-identifiable information is defined as information identifying an individual's registration with the Library or use of library materials or services. This includes all records, files, computers and electronic media that might contain such information.
>
> Patron-identifiable information refers to a wide-range of information maintained by the Library and includes any information that links a patron to use of Mount Prospect Public Library materials or services, or the patron's choices, taste, interest, or research. More broadly, patron-identifiable information is any information which:
>
> a. Refers to a patron by any identifiable characteristic (e.g. by name, address, telephone or other contact numbers, email address, identifying numbers such as library card number, license number or social security number);
>
> Or
>
> b. Provides, or could be used to determine, any information about a patron's library use.

This means all types of registration and circulation records and anything that contains registration and circulation records, including computers, computer components, disks and other electronic storage media, email, temporary internet files stored in a computer, computer sign-up sheets or other facility use logs, interlibrary loan requests and records, patron hold requests, or librarian notes pertaining to patron requests or assistance, and correspondence with patrons. Even records which do not include a patron's name, but refer to some other identifiable characteristic, such as the patron's library card number, contain patron-identifiable information and are subject to this policy.

Patron-identifiable information does not include statistical records relating to use of the Library or its materials and services that cannot be used to identify particular patrons. It also does not include information concerning behavioral issues (as distinguished from registration or circulation information) in the Library's records regarding a patron.[6]

Los Angeles Public Library

PII—any information relating to an identified or identifiable individual who is the subject of the information.

. . .

Anonymous information is information that does not identify specific individuals and is automatically transmitted by your browser.[7]

Musser Public Library

Confidentiality includes database search records, reference interviews, interlibrary loan records, computer use records, and all other personally identifiable uses of library materials, facilities or services.[8]

Princeton University Library (Quoting New Jersey Statutes: 18A:73-43.1)

"Library record" means any document or record, however maintained, the primary purpose of which is to provide for control of the circulation or other public use of library materials.[9]

Temple University Libraries

Library Records:

Records of the borrowing and use of library information resources (a.k.a. library materials) and equipment are considered to be confidential, as are the records of patron transactions of any type including, but not limited to, reference interactions, computer use logs, logs of Internet sites consulted, etc., as well as records of transactions regarding fees and fines. For library purposes, this covers all records related to the circulation or use of ipads, digital cameras, and any other equipment loaned by the University Libraries as well as books and other formats of printed or electronic information available from the Libraries, including materials that are personally owned by a faculty member that have been placed on reserve for reading in a course or of special collections materials donated or on deposit at the Libraries.

. . .

Collection and Security of PII

For certain defined business purposes the University Libraries do collect PII which data are individually or collectively sensitive or confidential according to current Temple University data classification. Both sensitive information and confidential information are held in strict confidence and exchanged among library staff or other University staff only in relation to the business purpose (i.e., on a need to know basis) and only by appropriately secure means.[10]

University at Albany Libraries

personal information: For purposes of this policy, "*personal information*" means any information concerning a natural person which, because of name, number, symbol, mark, or other identifier, can be used to identify that natural person.[11]

University of California Berkeley Library

Personally identifiable information is any information that can be directly or indirectly associated with a known individual. For example, all information contained in personnel, patron, and circulation files is personally identifiable.[12]

University of North Carolina at Chapel Hill Libraries (Quoting North Carolina General Statutes § 125-18)

"Library record" means a document, record, or other method of storing information retained by a library that identifies a person as having requested or obtained specific information or materials from a library. "Library record" does not include non-identifying material that may be retained for the purpose of studying or evaluating the circulation of library materials in general. (1985, c. 486, s. 2.)[13]

Syracuse University Libraries

> **"Individual Information"** includes personal name, physical addresses (including permanent and temporary residence addresses), electronic addresses (including e-mail, instant messaging addresses or screen names, and VOIP addresses or screen names), telephone numbers, and social security number.[14]

University of Texas Libraries

> University of Texas Libraries policy is that its circulation records and other records linking a library user with specific materials or services are confidential in nature.[15]

Documents associated with ALA's privacy advocacy efforts and its extensive Privacy Tool Kit discuss a variety of data and hosting systems that should fall under the auspices of library privacy policies. The documents include various privacy checklists and ancillary documents that reference systems and data, including the following:

- E-books and associated digital content (and associated features that gather personal information).[16]
- Library management systems, integrated library systems, and library websites, OPACs, and discovery services.[17] These include data such as
  - purchase-request data
  - personal identification data such as name, address, e-mail address, birth date, and so on
  - transactional data such as items borrowed and interlibrary loan requests and fulfillments, holds placed, and incurred fees and fines
  - personalization features offered by modern systems such as histories and lists of items checked out, favorite titles, and other reading lists
  - publicly shared data on materials such as user comments, ratings, recommendations, and reviews
  - website assessment, metrics, and analytics data
  - various data that can be contained in patron record free-text fields
- Public access computers and networks.[18] These include
  - the networks themselves—for example, Wi-Fi networks—and associated network applications such as proxy servers and other authentication systems
  - server logs associated with standard HTTP transactions
  - client computer and browser data such as cookies, downloaded content, saved files, browsing histories, and other cached data
- Third-party applications and content in general, whether unique to library operations or otherwise, including social media applications (and associated scripts and embedded content that can collect user information).[19]
- Video camera surveillance footage.[20]
- System backup content.[21]
- Other library-centric information such as
  - data associated with reference questions and interviews[22]
  - records or registration data that may be associated with the use of library programs and facilities and equipment[23]
  - e-mail notifications[24]
  - computer sign-up sheets[25]
  - other miscellaneous data

Some analyzed policies made no reference whatsoever to any particular systems involved in the collection or retention of private information; others provided more substantive detail. In sum, the following items, listed in no priority order, were mentioned in one or more of the library privacy policies analyzed.

Systems and Technologies Referenced

Integrated library systems, OPAC, "circulation system." Some policies mention the system by vendor name or vendor product name (such as Ex Libris or OverDrive) or by the locally branded name the library uses for its instance of the platform. In some cases, the platform (and associated services) are more generically referenced as *search and discovery platforms*. In some cases, particular item categories were mentioned, such as *use of audiovisual materials, films, or records*.

Electronic databases and journals. Such resources are mentioned by a variety of descriptors across the multitude of policies, such as *external*, *subscription*, *licensed*, *3rd party*, or, more generically, *external e-resource vendors* or *library subscription resources*. Similarly, some policies also reference *A–Z lists* (of databases or e-journals).

Research guides. These are mentioned generically as such, or in some instances referenced specifically by vendor name, such as Springshare.

Reference queries and virtual reference systems. Reference transaction methods and systems mentioned include *phone, mail, text, e-mail, instant messaging* or *chat,* and *in-person transactions.* Some policies mention the specific vendor platform name, such as QuestionPoint.

Institutional repositories. Sometimes institutional repositories are referenced by vendor platform, such as bepress's Digital Commons.

Interlibrary loan
Document delivery
Reserves
Online learning systems
Reservation systems (for example, for booking study rooms or computer use or for scheduling consultations)
Special collections registration forms
Generically, phrases such as *library applications, systems, and websites*. These could also include third parties, for example, *third-party vendors with whom the library has contracted services necessary for conducting business*.
E-mail
Analytics programs. In some cases, particular platforms are referenced by name, such as Google Analytics or Facebook Insights.
Websites and web server logs. References range from the more localized server and application logs that libraries hosting their own web server would possess to more generic and broader references, such as *external web resources or websites* (and whose server and application logs the local library would not host nor necessarily have access to).
Other types of log or history files. Related to the above items, references include logs of internet sites consulted and e-resource logs. Regarding local client computer information, items referenced include local application data such as that saved through use of web browsers (e.g., cookies, web history, and cached files). It could also include history information as found on tablets or e-readers circulated by the library.
Web forms. These often include references to surveys and questionnaires used for reference questions, feedback forms, or gathering assessment data.
Network infrastructure. These include references to such items as wireless access points and cell phones pinging their presence to the network infrastructure or other particular network applications, such as proxy servers.
Miscellaneous, including

- public network print management systems
- electronic or hard copy data related to photocopies or requests for photocopies
- software programs to monitor network traffic
- web-based management tools
- security camera video surveillance systems, tapes, and logs
- card swipe systems or other entry and exit physical building access systems
- online advertising platforms, including references to such platforms as Google Adwords and Facebook ads and programs such as the Amazon Services LLC Associates Program
- web beacons
- RFID

References to Particular Data Fields

Broadly speaking, references to particular data fields include typical patron record types of data, such as address information, financial information, and circulated item data, as well as a substantial number of other data types, some specific to core library-centric transactions, others not as much. In no particular order, data fields referenced within one or more of the analyzed policies included the following:

- name
- online platform screen name (such as an instant messaging or screen address)
- physical address (including various address fields, such as home address or shipping address)
- e-mail address
- phone number, fax number
- driver's license number
- library card number
- university ID number
- university or school status information (This includes references to such things as university major, university status, school, and education level.)
- grades (for credit courses taught by the library)
- specific employment fields related to library student workers
- Social Security number
- age (this includes references to age, age level, birth month and year, and birth date)
- gender
- preferences-related information or features
  - These include references to such things as preferences; reading preferences; reading habits; interests; favorites; and more generically, information and opinions about books, movies, music, and other topics; information about the patron's choices, taste, interest, or research; and hobbies.
  - In some cases, particular platforms are mentioned, such as references to the My Shelves functionality, a feature found in the BiblioCommons platform (used by several public libraries included in this study and whose privacy policy is incorporated onto those libraries' websites). Generically, references are made to website or application personalization features.
- interactive shared content (associated with online messaging applications, forums, and collaborative guides)
- circulation-related information (This includes references to such things as items currently checked out; checked-out item history; dues and fines presently due; fine history; items requested; canceled holds; and materials borrowed through interlibrary loan or document delivery.)

- materials ordering or collection development information (This includes data related to requests to order materials or actual order information for physical or electronic materials [such as books]; in some cases, the phrasing is broad, such as *information associated with the purchase of materials or collected and gathered for collection development purposes*.)
- computer and network use and browsing information
  This broad category includes data such as
  - searches done on library computers; information accessed through the internet; database search records; information about content explored or used such as websites visited
  - computer use; customer's use of a specific computer; computer guest pass distribution data; network ID information; authentication log-on credentials or log-on records
  - temporary internet files stored on a computer; workstation caches
  - items specifically relating to Wi-Fi usage, such as checkout information related to Wi-Fi hotspots and total data usage on the hotspot (and, in at least one case, specific mention of the Sprint telecommunications network and terms of use)
  - data fields contained in web server logs, such as internet domain information, IP address, type of browser and operating system used, date and time of access, pages visited, referring URL, and clock stream patterns
- online (or hard copy) registration and patron use data on items such as the use of library meeting rooms, facilities, or services; sign-up information for library classes and events
- assessment project data (This includes data on assessment projects dealing with topics such as services, collections, facilities, or other resources; it also includes demographic information often associated with such assessment projects.)
- citizen comment at a board meeting
- data about what website ad was viewed
- free-text data (such as feedback, suggestions, complaints, whether through an online form or hard copy)
- information related to use of special collections (This includes references to data associated with researcher request forms; permission to publish forms; permission to exhibit forms; duplication request forms; research interest or purpose for utilizing materials contained in special collections.)
- financial and donor information (This includes references to data on library donations, such as donor names, lists, and records; taxpayer ID number; credit card number and associated information [such as that collected for fines, specialized library services, or workshop registrations]; and billing address information.)
- reference transaction information (This includes references to online reference transactions; reference interviews [including notes taken during the interview process]; virtual reference chat transcripts and online conversations.)
- voice mail
- backup data contained on physical media (e.g., tape backups)
- security videos

Links to Third-Party Native Privacy Policies

A few library privacy policies provide links to the external privacy policies of vendors whose products they use to provide some service or content. A notable academic library example is found in the University of Denver's privacy policy, which provides direct links to a half dozen vendor privacy policies associated with external applications utilized by the library, such as Ex Libris and Springshare.[26] A notable public library example is Durham County Library, whose library policy provides links to the external privacy policies of over twenty external vendors that provide some service or content, including databases, online learning classes, e-books, online chat or e-mail reference services, and more.[27] San José Public Library stood out in terms of providing an abundance of direct links to external vendor privacy policies; this information is provided on a separate library webpage titled "Vendor Privacy Policies."[28] This page provides links to vendor policies organized by the following headings:

- eBooks & eMedia—fifteen vendor policies
- eLearning & eResearch—twenty-eight vendor policies
- On Our Website—twelve vendor policies (core library services such as the library catalog vendor, interlibrary loan application vendor, etc.)
- Other—three vendor policies (other miscellaneous services used by the libraries)

In addition, the library's web page provides additional links to opt-out instructions for several platforms.

A brief description of how some library policies choose to organize or describe broad categories of data is provided below.

Indiana University Libraries

Indiana's policy has a section stating, "Information that the IU Libraries may gather and retain about current and valid library users includes, but is not limited to, the following," and then proceeds to list information within eight topical categories, such as

"circulation information," "library surveys/assessment projects," and "user registration information."[29]

Middlebury Library

Middlebury's policy has a section titled "Privacy of Library Records" that includes the statement, "The library understands 'patron records' to include (but are not limited to) the following," followed by seven categories of data, such as "borrowing histories," "database searches," and "reference queries."[30]

Southern Illinois University Morris Library

SIU's policy includes a section titled "Information That Morris Library May Gather and Retain about Library Patrons Includes," which is then followed by eleven broad categories, such as "circulation services," "electronic resources," and "Special Collections Research Center." These categories are either types of information that may be collected or the entities within the library where that data may be collected. Each entry has additional information that includes examples of specific data types that may be collected.[31]

Syracuse University Libraries

Syracuse's policy includes a section titled "Definitions," which provides descriptions of five broad categories of information gathered—including "individual information," "authenticated services," and "business transactions." The policy also quotes New York state law, listing seven types of specific library records that are protected. The policy section "Details on Libraries' Information Gathering" notes nine specific services or areas where information may be gathered, including "browsing the libraries website," "technology loan," and "libraries research initiatives." Finally, the section "Summary" provides a chart that "summarizes the Libraries' information gathering practices" by service name, service type, and whether individual or university information is required to utilize the service.[32]

University of Denver Libraries

Denver's policy includes examples of transactional operations that produce data and the types of data that may be generated and collected. These include transactional instances such as "when you check out print materials," "when you use our facilities," and "when you use any portion of our website."[33]

Berkshire Athenaeum

One of Berkshire Athenaeum's several privacy-related policies, "Guidelines for Confidentiality While Cooperating with Law Enforcement," includes a section titled "Information Access and Confidentiality."[34] This section details nine types of records, systems, and transactions that can generate or maintain confidential information, such as "database search records," "circulation records," "reference interviews," and an extensive section on "public internet workstations," which discusses the library's use of a computer reservation management program and print management program, among other things.

Beaufort County Library

One of Beaufort County Library's privacy-related policies, its "Privacy and Confidentiality Policy," provides over a dozen examples of records protected by South Carolina law.[35] It also provides examples of specific data fields that are protected, such as names, addresses, phone numbers, and so on.

San José Public Library

San José Public Library's "Privacy Policy" details California state law and lists some data fields protected by law.[36] The section "What information do we collect?" lists over a dozen data fields for which information may be collected when using library services (e.g., name, address, date of birth, items currently checked out, etc.). The policy also covers other items, such as Google Analytics, web browser information, reservation statistics, circulated tablet and e-reader device histories, e-mail, RSS feeds, and video security cameras. Another section, called "Using third-party vendors," discusses the use of third-party vendors to provide several library-related services and content, including digital collections, streaming media content, and so on, and discusses the types of information such third-party services may collect. This information is in addition to that on the "Vendor Privacy Policies" web page mentioned earlier.

Notes

1. American Library Association, *Privacy: An Interpretation of the Library Bill of Rights* (Chicago: American Library Association, 2002, amended 2014, 2019), 1, www.ala.org/advocacy/sites/ala.org.advocacy/files/content/intfreedom/librarybill/interpretations/privacyinterpretation.pdf.
2. American Library Association, *Code of Ethics of the American Library Association* (Chicago: American Library Association, 1939, amended 1981, 1995, 2008), www.ala.org/advocacy/sites/ala.org.advocacy/files/content/proethics/codeofethics/Code%20of%20Ethics%20of%20the%20American%20Library%20Association.pdf.
3. American Library Association, "Privacy," last updated April 2017, www.ala.org/advocacy/privacy.
4. American Library Association, "Privacy and Confidentiality Q&A," last updated July 29, 2019, www.ala.org/advocacy/intfreedom/privacyconfidentialityqa.
5. Hutto Public Library, "Confidentiality of Library Records," *Policies and Procedures Manual* (Hutto, TX: Hutto Public Library, 2008, rev. 2015, 2016, 2017, 2018), 19, https://cms.revize.com/revize/huttotx/030%20Library%20Policies%20%20Procedures%202018_approved%20by%20City%20Council%204-19-2018.pdf.

6. Mount Prospect Public Library, "Privacy and Confidentiality of Patron Information Policy," https://mppl.org/wp-content/uploads/2011/08/Privacy-Policy-111716.pdf.
7. Los Angeles Public Library, "Online Privacy Policy," last updated March 2018, https://www.lapl.org/online-privacy-policy.
8. Musser Public Library "Confidentiality Policy," August 19, 2015, https://musserpubliclibrary.org/wp-content/uploads/2018/08/Confidentiality-Policy.pdf.
9. Princeton University Library, "Patron Confidentiality," http://library.princeton.edu/services/access/policies/confidentiality.
10. Temple University Libraries, "Confidentiality of Patron Records," last updated January 31, 2017, https://library.temple.edu/policies/confidentiality-of-patron-records.
11. University at Albany Libraries, "Internet Privacy Policy," https://library.albany.edu/privacy.
12. University of California Berkeley Library, "Collection, Use, and Disclosure of Electronic Information," last updated September 22, 2008, https://www.lib.berkeley.edu/about/privacy-electronic-information.
13. University of North Carolina at Chapel Hill Libraries, "Privacy Policy," last updated March 19, 2018, https://library.unc.edu/about/policies/privacy-policy/.
14. Syracuse University Libraries, "Privacy Policy," version 2.0, last updated October 4, 2013, https://library.syr.edu/policy/documents/privacy-policy.pdf.
15. University of Texas Libraries, "Privacy and Confidentiality of Library Records Policy," https://www.lib.utexas.edu/about/policies/privacy-and-confidentiality-library-records-policy.
16. American Library Association, "Library Privacy Checklist for E-Book Lending and Digital Content Vendors," last updated January 26, 2020, www.ala.org/advocacy/privacy/checklists/ebook-digital-content.
17. American Library Association, "Library Privacy Checklist for Library Management Systems/Integrated Library Systems," last updated January 26, 2020, www.ala.org/advocacy/privacy/checklists/library-management-systems; American Library Association, "Library Privacy Guidelines for Library Management Systems," last updated January 26, 2020, www.ala.org/advocacy/privacy/guidelines/library-management-systems; American Library Association, "Library Privacy Checklist for Library Websites, OPACs, and Discovery Services," last updated January 26, 2020, www.ala.org/advocacy/privacy/checklists/OPAC; American Library Association, "Library Privacy Guidelines for Library Websites, OPACs, and Discovery Services," last updated January 26, 2020, www.ala.org/advocacy/privacy/guidelines/OPAC.
18. American Library Association, "Library Privacy Checklist for Public Access Computers and Networks," last updated January 26, 2020, www.ala.org/advocacy/privacy/checklists/public-access-computer; American Library Association, "Library Privacy Guidelines for Public Access Computers and Networks," last updated January 26, 2020, www.ala.org/advocacy/privacy/guidelines/public-access-computer.
19. American Library Association, "Library Privacy Guidelines for Library Websites."
20. American Library Association, "Video Surveillance in the Library Guidelines," approved June 8, 2020, www.ala.org/advocacy/privacy/guidelines/videosurveillance.
21. American Library Association, "Developing or Revising a Library Privacy Policy," Privacy Tool Kit, last updated April 2017, www.ala.org/advocacy/privacy/toolkit/policy.
22. American Library Association, "Developing or Revising."
23. American Library Association, *Privacy: An Interpretation of the Library Bill of Rights*.
24. American Library Association, "Privacy."
25. American Library Association, "Privacy."
26. University of Denver Libraries, "Your Privacy and University Libraries," https://library.du.edu/policies/records-privacy.html.
27. Durham County Library, "Privacy Policy," July 2019, https://durhamcountylibrary.org/about/policies/privacy-policy/.
28. San José Public Library, "Vendor Privacy Policies," last updated August 12, 2019, https://www.sjpl.org/vendor-privacy-policies.
29. Indiana University Libraries, "Indiana University Libraries Privacy Policy," last updated February 1, 2012, https://policies.iu.edu/policies/lib-01-libraries-privacy/index.html.
30. Middlebury Library, "Privacy and Security of Library Records," https://www.middlebury.edu/library/about/policies/privacy-security.
31. Southern Illinois University Morris Library, "Patron Privacy Policy," December 2, 2015, https://lib.siu.edu/about/policies/patron-privacy-policy.php.
32. Syracuse University Libraries, "Privacy Policy."
33. University of Denver Libraries, "Your Privacy."
34. Berkshire Athenaeum, "Guidelines for Confidentiality While Cooperating with Law Enforcement," 2010, https://static1.squarespace.com/static/5c7eed16e8ba44443d295e02/t/5cb177cdeb39315a7ce00238/1555134414545/BA_LawEnforcement_Confidentiality.pdf.
35. Beaufort County Library, "Privacy and Confidentiality Policy," 2019, https://2f26905f-7709-4fc5-8602-f82d730cafe1.filesusr.com/ugd/a57334_90d2a4c4428a4ea89dbfa0b3c5e12699.pdf.
36. San José Public Library, "Privacy Policy," last updated March 12, 2018, https://www.sjpl.org/privacy-policy.

Chapter 3

Why Data Is Collected and How It Is Used

A vast majority of the analyzed policies provide some rationale as to why the library collects data and how it is used. Some policies provide broad umbrella statements, conceivably covering a whole range of systems, data, and transactions. Others include such statements but also provide further detail on one or more particular systems, transactions, or data types. ALA's "Library Privacy Checklist—Overview" notes that library policies should "specify that the library is not collecting more user information than what it needs" and should "[include] information about what information the library is tracking, why, and for how long the data is kept."[1] ALA's *Resolution on the Retention of Library Usage Records* notes that because "library usage records containing personally identifiable information (PII) are maintained for the sole purpose of effectively managing library resources," libraries should "limit the degree to which personally identifiable information is collected, monitored, disclosed, and distributed" and "avoid creating unnecessary records."[2]

As noted in many policies, libraries collect data in association with the library fulfilling its core business and administrative responsibilities of providing access to library resources and services. This chapter provides policy statement examples for both levels of detail—broad and overarching statements, and granular and specific statements. To begin, many library policies incorporate some level of overarching phrasing (some examples of which are provided in the ALA Privacy Tool Kit). For example, Rutgers University Libraries' policy notes,

> The Rutgers University Libraries gather information about current and valid library users for the sole purpose of providing library services. Where it is necessary for the Libraries to identify users, it is our goal to gather only the minimum information necessary and to retain that information for only as long as it is needed to complete a particular transaction. We avoid creating unnecessary records and retaining records not needed for the fulfillment of the mission of the Libraries. Furthermore, we do not engage in practices that might place personally identifiable information in or on public view.[3]

Additional broad, high-level statements noting data collection associated with fulfilling library operational requirements are provided below (and in some of the instances below, the library's policy later provides greater detail on one or more data types):

Colby College Libraries

> We do not collect information about patron activities . . . beyond what is basic and necessary to conduct and fulfill the mission of the library.[4]

California Polytechnic State University Robert E. Kennedy Library

> To aid understanding of the use or value of resources and services, the Kennedy Library may aggregate and retain user data for a reasonable period of time. It will, however, neither collect nor retain information identifying individuals except for the purpose of furnishing a specific service.[5]

Northeastern University Library

> The Libraries collect information about visitors and visits for statistical purposes, to administer access to Library materials and services, and to inform users of Library services and programs.[6]

Temple University Libraries

> For certain defined business purposes the University Libraries do collect PII which data are individually

> or collectively sensitive or confidential according to current Temple University data classification. Both sensitive information and confidential information are held in strict confidence and exchanged among library staff or other University staff only in relation to the business purpose. . . .
>
> PII collected is made accessible only to those specific individual staff who need access to the information in order to conduct library business or who will be compiling and anonymizing data for statistical or assessment purposes.[7]

University of Chicago Library

> In order to conduct Library business, the Library collects and maintains personally identifiable information about library users. . . .
>
> Identifiable information may be retained, in some cases indefinitely, when doing so serves an institutional purpose.[8]

University of Michigan Library

> The University of Michigan Library may collect some data about your library use in order to improve services and to integrate with broader University teaching and learning initiatives.
>
> . . .
>
> When you use library applications, systems, and websites, you generate data. We use and store these data to provide and improve services and resources.[9]

Syracuse University Libraries

> The Libraries provide a vast array of services. Many services do not require users to divulge any information to Libraries staff or systems. Other services, however, require users to provide some information in order to receive or benefit from the service.[10]

Brooklyn Public Library

> All library records that identify patrons by name are strictly confidential, and access to them is limited to staff for legitimate library business.[11]

Jessamine County Public Library

> The Jessamine County Public Library acts to limit the amount of personally identifiable information it retains. Some information, however, is necessarily and understandably retained for the transaction of day-to-day business.
>
> Most information related to customers is kept for the purposes of circulating materials and ensuring that responsibility is attributed to the correct person when an item is borrowed.[12]

Mount Prospect Public Library

> Staff should create records with patron-identifiable information only as reasonably necessary for the Library's operations.
>
> Staff should consult records with patron-identifiable information only for legitimate purposes related to the Library's operations.[13]

Pierce County Library System

> Information and usage records with personally identifiable customer information are maintained for the purpose of effectively managing library resources and providing library services.[14]

Several policies reference or directly quote state law, which in some instances itself directly speaks to the purpose and use of some data collected by a library within that state. For example, Princeton University Library's policy notes, "As required under New Jersey law (N.J. Stat. § 18AG73-43.1 – 43.2), Princeton University Library records relating to an individual patron's use of the Library and its resources shall be treated as confidential," and then quotes the relative New Jersey statute section passage that speaks to how library records can be "necessary for the proper operation of the library."[15] Deer Park Public Library's policy quotes New York Civil Practice Law and Rules, Section 4509, which also references how records can be used "for the proper operation" of the library: "Library records, which contain names or other personally identifying details regarding the users . . . may be disclosed to the extent necessary for the proper operation of such Library."[16]

Geauga County Public Library references Ohio Revised Code Section 149.432, which notes that a library record includes

a) Information that the library requires an individual to provide in order to be eligible to use library services or borrow materials;

b) Information that identifies an individual as having requested or obtained specific materials or materials on a particular subject;

c) Information that is provided by an individual to assist library staff answer a specific question or provide information on a particular subject.[17]

Las Vegas–Clark County Library District's policy references Nevada Revised Statutes NRS 239: "In accordance with NRS 239, the District will not retain any records pertaining to a patron's use of library resources longer than necessary to provide appropriate stewardship of those resources."[18]

Moving to examples of policy statements providing more detail on how particular data may be used, Duke University Libraries' policy concludes with a section titled "Examples of How the Libraries Use Data to Improve Services." This section provides details and accompanying data graphs that help illustrate how library staff utilize textbook circulation data, interlibrary loan request data, physical space swipe entrance data, Google Analytics data, and data analyzed from their EZproxy proxy server logs.[19] The rest of this chapter will share policy statement examples regarding the following types of data and how and why such data is collected and in the process will surface a rich variety of policy phrasing, nuance, and focus:

- web server logs and associated analytics data
- cookies
- electronic resource usage and logs
- e-mail and web forms
- virtual reference transactions, including components such as chat transcripts
- survey data
- core patron and circulation records typically managed by a library services platform or integrated library system
- interlibrary loan and document delivery data
- authentication services and computer use data
- social media
- donors
- video camera surveillance footage
- photos and videos (not related to surveillance)
- various miscellaneous data

Web Server Logs and Analytics

Web server logs, their associated analysis through analytics programs such as Google Analytics, and other data related to the library website represented the single most mentioned data or record type with an associated reason provided for such collection. Some level of detail appeared in at least twenty-two of the academic library policies and a dozen public library policies. Phrasing can vary significantly, but many focus on common threads of collecting and using such data to assist with troubleshooting issues, to better understand and meet the needs of users (e.g., improving the website), and for statistical purposes.

University at Albany Libraries

> The information that is collected automatically is used to improve this Web site's content and to help the University Libraries understand how *users* are interacting with its Web site. This information is collected for statistical analysis and to determine what information is of most and least interest to our *users*.[20]

Indiana University Libraries

> Web site developers and owners review usage data on their web pages to identify resources that are being used and to evaluate the provision of information on the site and the effectiveness of the organization and design of that information.[21]

Syracuse University Libraries

> The Libraries use this information to track site usage, monitor site performance, and generate aggregate statistics.[22]

San Diego State University Library

> The Library may record aggregated data (stripped of identifying characteristics) on website and resource usage in order to improve website usability and collection relevance.[23]

University of Miami Libraries

> The UM Libraries' web servers may also use browser "cookies" or other technologies to maintain session and preference information and to provide other complex functionality. The Library will use cookies to capture IP addresses for collecting data on web usage.[24]

University of Chicago Library

> This automatically collected information is only used internally for technical troubleshooting, to monitor compliance with the Library's Policy on Acceptable Use of Electronic Resources, to improve the usability of our website, and to record aggregate statistics.[25]

University of North Carolina at Chapel Hill Libraries

> For site administration functions, information, other than personal information linked to a particular individual, is collected for analysis and statistical purposes of Web site navigation. This information is used to help diagnose problems, assess what information on the sites is of most interest,

> determine technical design specifications, identify system performance and/or problem areas, and other administration functions.
>
> . . .
>
> Our use of tracking technologies allows us to analyze trends and statistics to improve our Web site and your Web experience.[26]

University of California Berkeley Library

> In the course of providing you with Web-based services, The Library collects and stores certain information automatically through our Web site. We use this information on an aggregate basis to maintain, enhance or add functionality to our Web-based services.[27]

University of Michigan Library

> The U-M Library also uses Google Analytics (including the use of demographics and interest reports), a web analytics service provided by Google, Inc. ("Google") to help understand how U-M Library websites are being used and to improve our interface and services. . . .
>
> The U-M Library uses this information for analytical and feature-improvement related purposes only.[28]

Villanova University Falvey Memorial Library

> We routinely collect information from website usage to help us improve functionality, navigation, and performance.[29]

University of Oregon Libraries

> When users visit our website, we may automatically collect certain information. . . . This is standard practice for websites, and is not used for any purpose other than to evaluate how we can design the site to best serve user needs.[30]

Auburn University Libraries

> We use non-identifying and aggregate information to better design our services. For example, we may let it be known publicly that a specific number of individuals visited a certain area on our website, but we would not disclose anything that could be used to identify those individuals.[31]

Atlanta-Fulton Public Library System

> This information is collected for statistical analysis using third-party or proprietary software programs to create summary statistics. The statistics are used for the purpose of determining what information is of most and least interest to all visitors and for identifying system performance issues or problem areas in order to better plan future portal enhancements.[32]

Berkshire Athenaeum

> The Berkshire Athenaeum will collect and store only the information necessary to measure the number and timing of visitors to different areas of the Athenaeum's website to assist in making these sites more useful.[33]

Lower Macungie Library

> Statistical Information: This information is used by the Lower Macungie Library for the operation of the service, to maintain quality of the service, and to provide general statistics regarding use of Lower Macungie Library web sites.[34]

Mount Prospect Public Library

> We use your IP address to help diagnose problems with our server, and to administer and create generalized statistics on our Web site. We may also use an IP address to block abusive users of public forums.[35]

Nashville Public Library

> The library and its third party vendors do keep track of how users navigate our web sites: which pages are most frequently used, popular search paths, domains of users (to find out where our users are visiting from), and other information that helps us make adjustments and improve our service. This information is not shared, and is used by us for general and not individual statistics.[36]

Ann Arbor District Library

> **Log Files**
>
> When a user visits our website, his/her IP address is recorded. We use this information to analyze trends, administer the site, determine popularity of content, and gather broad demographic information for aggregate use.[37]

Phoenix Public Library

> Statistical Information: Phoenix Public Library collects information to maintain the quality of its services and to report aggregate information on the usage of its website to City management, as well as state and federal agencies and national library organizations.[38]

Queens Borough Public Library

> The Library uses this information to help the Library make our site more useful to visitors and to learn about the number of visitors to our site and the types of technology our visitors use.[39]

Cookies

Many library policies note the use of cookies and provide brief definitions of what a cookie is. Cookies can be used by website analytics programs, but for other purposes as well, as shown below:

Michigan State University Libraries

> This Site uses cookies for two main purposes: (a) to carry information about your current session at this Site from one web page to the next, which also allows you to automatically login to other Michigan State University websites, and (b) to identify you on this Site on return visits.[40]

University of Oregon Libraries

> Users of networked computers will need to enable cookies in order to access a number of resources available through the Libraries. . . . Cookies are often used to remember information about preferences and pages visited. . . . Our library servers use cookies solely to verify that a person is an authorized user in order to allow access to licensed library resources.[41]

Josephine-Louise Public Library

> One of the primary purposes of cookies is to provide a convenience feature to save you time. The purpose of a cookie is to tell the Web server that you have returned to a specific page. . . . When you return to the same Josephine Louise Public Library—Walden, New York Web site, the information you previously provided can be retrieved, so you can easily use the Josephine Louise Public Library—Walden, New York features that you customized.[42]

Pierce County Library System

> Examples in which the Library might use cookies would be to customize content areas; to analyze site activity or user behavior; or to maintain the state of authentication for member privileged pages during a given session.[43]

Los Angeles Public Library

Los Angeles Public Library's Online Privacy Policy provides extensive detail on the types of information collected when a user visits the library's website. Notably, it also states,

> **How we use information collected on lapl.org for digital advertising of library services**
>
> **We utilize third-party tools for outreach**
>
> Our team and affiliates use third-party web services to conduct outreach and education through the use of digital advertising for the Los Angeles Public Library initiatives.[44]

It then proceeds to provide definitions for, and details on, the library's utilization of Google Adwords, Facebook Ads, Google Analytics, Hotjar cookies, web beacons, session cookies, persistent cookies, click tracking, conversion tracking, retargeting, and targeted advertising. It notes why the library uses these technologies as well as methods to opt out of data collection.

Other References Related to Electronic Resource Usage and Logs

A few library policies make references to data collection and use focused on assessing electronic resource usage, such as licensed library databases:

Penn State University Libraries

> Collection and analysis of data on usage of the licensed commercial online databases and materials offered by the Libraries through its system assists both the publisher and the University Libraries to understand the impact of this technology and service.[45]

Harvard Library

> Harvard does gather data about system and resource usage for administrative purposes. . . .
>
> The resulting logs contain information necessary for analyzing the use of resources, troubleshooting problems and improving services.

> Log data is also used to distribute resource costs among Harvard libraries and faculties.[46]

Syracuse University Libraries

> The Libraries may use information that they collect about online database use for internal business purposes and to improve the Libraries' services.[47]

University of Denver Libraries (in reference to their EZproxy proxy server logfiles)

> We may use these logs to troubleshoot authentication errors or prevent and/or stop security breaches when they occur. We may also anonymize and analyze these logs in order to assess our collections and their use.[48]

E-mail and Web Forms

Several policies discuss collection and use of data associated with e-mail and web forms. Examples include the following:

Auburn University Libraries

> We use e-mail addresses to respond to the e-mail we receive, to send library notices, to confirm online program registrations, and occasionally to alert customers to new services they may want to use. Mailing addresses may be used to send library-related notices. Such addresses are not used for any other purpose and are not shared with outside parties.[49]

University at Albany Libraries

> Your e-mail address and the information included in your message will be used to respond to you, to address issues you identify, to improve this Web site, or to forward your message to another SUNY campus for appropriate action.[50]

University of Chicago Library

> If you choose to submit personally identifiable information to the Library (through web forms, email messages, or other communication), that information will be used only for the purpose for which you submitted it, with the exception that the Library may make reasonable statistical reports that do not identify particular individuals.[51]

University of Denver Libraries

> We may collect e-mail addresses and other contact information, in order to provide and improve our services.
>
> . . .
>
> If you fill out an electronic form on our site, such as those for reporting a problem, reserving study rooms, requesting a consultation, asking a question, etc., we keep these data in order to troubleshoot, improve services, and/or to keep statistics on our work.[52]

Pierce County Library System

> The Library may use personally identifiable information to contact you for promotional purposes. For example, on occasion the Library may wish to send e-mails to inform you of new exhibitions or other events the Library deems may be of interest. You will not receive such communications unless you have willingly provided your personal contact information.[53]

Queens Borough Public Library

> Personally identifying information that you provide by e-mails or web forms will be used only for such purposes as are described at the point of collection (for example on a web form), such as to send information or provide library services to you, update your membership record, or to respond to your questions or comments.
>
> If you provide contact information, the Library may contact you to clarify your comment or question, or to learn about your level of customer satisfaction with library services.[54]

San José Public Library

> Any personal information given in email messages, chat sessions, web forms, in-person or telephone reference, or other communications is only used for the purpose for which you submitted it.[55]

Virtual Reference Transactions

As evidenced above, some policies specifically note how e-mail can be used for reference services. Several library policies provide further details related to virtual reference services (such as chat transcripts), and some libraries have dedicated virtual reference service policies, such as Texas State University Libraries.

Duke University Libraries

> The Libraries collect and store personal information that you submit via the Libraries' web-based management tools, such as forms related to asking reference questions or booking reservable study rooms.

> We also interact with our library users regularly and receive personal information via email messages, chat sessions, web forms, and other communications. If you submit personal information via one of these platforms, we use your personal information only for the purpose for which you submitted it.[56]

Middlebury Library

> We access these transcripts to evaluate the quality of our service and for statistical purposes.[57]

Temple University Libraries

> These transcripts are restricted for the purposes of internal training, statistical reporting, and may at times be repurposed, once stripped of any identifying information. . . .
>
> The transcripts are analyzed for the amount and types of questions we are being asked. This helps determine appropriate staffing levels and aids in training librarians to staff the reference service. Frequently asked questions may at times be mined and repurposed in order to populate the FAQ knowledge-base, but no identifying information is made public.[58]

Texas State University Libraries

- The Alkek Library Ask a Librarian service records all reference transactions, including the chat conversation and the URLs for all the web sites visited.
- At the end of the session, you have the option to have the transcript emailed to you and a copy will be stored in our database for a period of one year.
- Transcripts maintained by the library will be used for assessment and training purposes only.
- We will not disclose any personal data we collect from you to any other party in a manner that would identify you, except where required by law, or in order to fulfill your service request.[59]

Syracuse University Libraries

> The Libraries may use information they collect during reference transactions for internal business purposes and to improve the Libraries' services.[60]

Surveys

Several policies discuss data collected through surveys, oftentimes associated with user assessment activities.

Syracuse University Libraries

> **Libraries Research Initiatives:** In order to improve their service to the community, the Libraries occasionally may conduct survey studies, issue questionnaires, or perform other data gathering activities. During these initiatives, the Libraries may ask visitors to provide Individual Information or University Information. In these circumstances, the Libraries consider this information optional; the visitor or user can choose whether or not to provide this information. Further, a visitor's decision to withhold Individual Information or University Information from a Libraries employee who is conducting a research initiative will not harm, diminish, or otherwise affect the level of service that visitor receives from the Libraries.[61]

University of North Carolina at Chapel Hill Libraries

> **Library Surveys and Assessments**
>
> Periodically, The University of North Carolina at Chapel Hill Libraries conduct library surveys and assessments. Information and data obtained through electronic, group or individual surveys are considered confidential and will adhere to Institutional Review Board policies, as appropriate, unless otherwise publicly stated in the collection process or permission is explicitly obtained from the respondent(s).
>
> Periodically, the libraries review and use demographic and similar aggregated data for reports, both internal and external. This use does not identify individuals.[62]

Brown County Library

> Any information the library user chooses to provide, such as information gathered through voluntary library user surveys, will be used only to provide or improve library services.[63]

Josephine-Louise Public Library

> Josephine Louise Public Library—Walden, New York may also contact you via surveys to conduct research about your opinion of current services or of potential new services that may be offered.[64]

Lower Macungie Library

> Survey information is used for purposes of monitoring or improving the satisfaction of LML patrons.[65]

Patron Records and Circulation Services

Patron identification data (e.g., name, address, etc.) and collecting this information to establish a patron record allowing the circulation of materials and the providing of other services is frequently mentioned in policies.

Duke University Libraries

> The Libraries maintain personally identifiable information in library users' online accounts. . . . We use this information to maintain your library account and to provide services to you.[66]

Montana State University Library

> If you wish to receive borrowing privileges, we must obtain certain information about you in order to provide you with a library account.[67]

Texas Tech University Libraries

> We will use the personally identifiable information only to maintain your library account and respond to your requests.[68]

Syracuse University Libraries

> The Libraries require all users to provide University Information in order to borrow materials from the Libraries, including books and laptop computers.
>
> The Libraries may use circulation information they collect for internal business purposes and to improve Libraries services.[69]

Fairbanks North Star Borough Public Libraries

> The library maintains a confidential database of its users which includes information for personal identification, as well as any library items currently checked out to that borrower. . . . Collection and maintenance of this information is necessary so that the library can account for Borough property.[70]

Geauga County Public Library

> Circulation records and other records identifying the names of library users with specific materials are retained while the materials are charged to a patron and when materials are returned until of no further administrative value.[71]

Las Vegas–Clark County Library District

> In order to provide borrowing privileges, the District must obtain certain information about its patrons.[72]

Interlibrary Loan and Document Delivery Services

Interlibrary loan and document delivery services data are also mentioned in several policies.

Cornell University Library

> Interlibrary Loan lending and borrowing records have been retained since at least 2001. They are used in case there are billing problems and to comply with the record keeping requirements suggested by the CONTU (National Commission on New Technological Uses of Copyright Works) guidelines. . . . In some cases, information about requests (including the name of the requestor) is shared within the library staff for collection development purposes, but staff are instructed not to further disseminate such information.[73]

University of California San Diego Library

> The Library also collects information in conjunction with Library Express, Interlibrary Loan, or San Diego Circuit patron requests submitted via Roger or Melvyl, to allow us to complete the requested service transaction for you.[74]

Authentication Services and Computer Use

User IDs and passwords associated with providing access to databases or logging on to a computer are mentioned in several policies.

Southern Illinois University Morris Library

> Use of the full resources of the World Wide Web and of the full power of some subscription databases requires that a user log on to the workstation.[75]

San Diego State University Library

> All SDSU affiliated patrons will be required to sign onto internet access terminals using their SDSUid. This is necessary to identify SDSU affiliates from community users and is done solely to be in compliance with legal contracts.[76]

Rutgers University Libraries

> When using library services through our website, you may need to provide your name, e-mail address, NetID, password, barcode, and/or password. To use licensed subscription electronic resources from an off-campus location, users are required to submit a NetID and password or library barcode and password to be authenticated as a currently affiliated user.[77]

Ann Arbor District Library

> In order to use the Internet stations at an AADL branch, a user must provide his/her name and address and show valid identification. This information is only used in the event that the user breaks one of the AADL rules of behavior during his/her session.[78]

Social Media

Several public library policies note how the libraries may use social media data.

Nashville Public Library

> By accessing NPL's blog and social media sites, as well as interacting with content there . . .
>
> **What You Should Know.**
>
> **The Library Owns the Content.**
>
> What This Means: NPL can use content without limits.[79]

Berkshire Athenaeum

> The Berkshire Athenaeum shall also be granted the right to reproduce comments, posts, and messages in other public venues. For example, a response to a YouTube book review may be quoted in a newspaper or on the library website.[80]

Jessamine County Public Library

> Many social media sites allow users of those sites to become a "friend," "fan" or otherwise associate their own "profiles" or virtual presences with the library's profile on these sites. The library does not collect, maintain, or otherwise use the personal information stored on any third party site in any way other than to communicate with users on the site.[81]

Donors

Several policies include specific references to donor-related data.

Ann Arbor District Library

> **Donating to the Library**
>
> When a donation is given to AADL, we will record the donor's name, address and type and amount of gift to comply with AADL auditing procedures and to issue the donor a receipt for tax purposes.[82]

Genesee District Library

> Donor lists may be used by Genesee District Library for ongoing communication and the solicitation of future gifts, in accordance with Michigan Law, unless the donor has stipulated otherwise.[83]

Video Camera Surveillance Data

Footage captured by video surveillance systems is frequently mentioned in policies, and several libraries have separate, individual policies focused on video surveillance.

Ocean County Library

> The Library uses surveillance cameras in some of its facilities to complement other measures to ensure a safe and secure environment for customers and staff. The equipment helps to protect the library's property against theft or vandalism and can assist in identifying intruders and persons breaking the law or violating the library's Rules of Conduct.[84]

Jessamine County Public Library

> The Library will use digital video to enhance the safety and security of Library customers, staff, and property, while protecting individuals' right to privacy. The primary use of security cameras is to discourage inappropriate and illegal behavior and to improve the opportunity to apprehend offenders.[85]

Alpha Park Public Library District

> Security cameras are in use to discourage illegal behavior and violations of library policies, and to provide recorded footage to assist law enforcement

in prosecuting criminal activity and staff in enforcing library policies.[86]

University of Oregon Libraries

> The University of Oregon Libraries (UO Libraries) values academic freedom and personal privacy, and employs security cameras only to the extent required to assist in protecting library resources and providing safety for library users.
>
> . . .
>
> Security cameras may be placed strategically in and around the UO Libraries to meet the specific needs of library departments and to assist the UO Police Department (UOPD) in its efforts to deter crime; protect library staff and patrons; protect facilities, collections and equipment; assist with emergency response situations; and investigate suspected criminal behavior.[87]

University of North Carolina at Chapel Hill Libraries

> Some campus libraries have security cameras installed to improve safety for patrons and staff and to help prevent theft and vandalism. These recordings are used by library staff and law enforcement officials investigating incidents that occur in the libraries.[88]

Photos and Videos for Promotional Purposes

Distinct from video surveillance footage, several public library policies reference promotional use of photos and videos.

Genesee District Library

> Photos and videos from general library scenes, public programs and events held in Library facilities and spaces may be used on the Library's website and/or in social media and publications.[89]

St. Louis Public Library

> The Library may utilize photos and videos from public programs and events at Library facilities and Library spaces on its website and in Library publications. Photos, images, and videos submitted to the Library by users for online galleries or contests may also be used by the Library for promotional purposes.[90]

Miscellaneous

Several policies address other miscellaneous types of data collected and how such data is used.

University of Denver Libraries

> We collect data regarding how many people enter/exit the building and peoples' usage of space during library operating hours. These data are anonymized. They are used to improve the design of physical space within the building.[91]

Ann Arbor District Library

> **Board Meetings**
>
> In order to make a citizen's comment at an AADL Board Meeting, a citizen will be asked to present his/her name and address. The information given will not be used in any other way.[92]

Notes

1. American Library Association, "Library Privacy Checklist—Overview," last updated January 26, 2020, www.ala.org/advocacy/privacy/checklists/overview.
2. American Library Association, *Resolution on the Retention of Library Usage Records* (Chicago: American Library Association, 2006), https://alair.ala.org/bitstream/handle/11213/1594/52.4.4%20Retention%20of%20Library%20Records.pdf.
3. Rutgers University Libraries, "Privacy Policy," October 19, 2010, https://www.libraries.rutgers.edu/privacy_policy.
4. Colby College Libraries, "What Are the Privacy Policies in the Library?" Guidelines and Policies, https://www.colby.edu/libraries/about/guidelines-and-policies/.
5. California Polytechnic State University, Robert E. Kennedy Library, "270.5.2 Privacy of Online Library Users," Campus Administrative Policies, Chapter 200, Academic Affairs, 270 Robert E. Kennedy Library, 2015, https://policy.calpoly.edu/cap/200/cap-270.
6. Northeastern University Library, "Privacy Statement," last updated December 21, 2011, https://library.northeastern.edu/about/visitors/visitor-policies-and-forms/privacy-statement.
7. Temple University Libraries, "Confidentiality of Patron Records," last updated January 31, 2017, https://library.temple.edu/policies/confidentiality-of-patron-records.
8. University of Chicago Library, "Privacy Statement," https://www.lib.uchicago.edu/about/thelibrary/policies/privacy/.
9. University of Michigan Library, "Library Privacy Statement," last updated March 2016, https://www.lib.umich.edu/library-administration/library-privacy-statement.
10. Syracuse University Libraries, "Privacy Policy," version 2.0, last updated October 4, 2013, https://library.syr.edu/policy/documents/privacy-policy.pdf.

11. Brooklyn Public Library, "Privacy Statement," https://www.bklynlibrary.org/use-the-library/policy/privacy-statement.
12. Jessamine County Public Library, "Information Security Policy," last updated August 21, 2019, https://jesspublib.org/wp-content/uploads/3.6-Information-Security-Policy-2019-09-25.pdf.
13. Mount Prospect Public Library, "Privacy and Confidentiality of Patron Information Policy," https://mppl.org/wp-content/uploads/2011/08/Privacy-Policy-111716.pdf.
14. Pierce County Library System, "Confidentiality of Library Records and Customer Files," last updated October 15, 2013, https://www.piercecountylibrary.org/about-us/policies/confidentiality-library-records.htm.
15. Princeton University Library, "Patron Confidentiality," http://library.princeton.edu/services/access/policies/confidentiality.
16. Deer Park Public Library, "Library Patron Records Confidentiality Policy," February 23, 2011, https://deerparklibrary.org/wp-content/uploads/2017/06/Library-Patron-Records-Confidentiality.pdf.
17. Geauga County Public Library, "Confidentiality and Storage of Patron Personal Information and Circulation Records," Geauga County Public Library Operating Policy Manual, last updated December 17, 2019, http://divi.geaugalibrary.net/wp-content/uploads/2020/01/710-Confidentiality-and-Storage-of-Patron-Circ-Records.pdf.
18. Las Vegas–Clark County Library District, "Patron Privacy Policy," last updated April 10, 2014, https://lvccld.org/wp-content/uploads/sites/54/2017/10/privacypolicy.pdf.
19. Duke University Libraries, "Duke University Libraries Privacy Statement," https://library.duke.edu/about/privacy.
20. University at Albany Libraries, "Internet Privacy Policy," https://library.albany.edu/privacy.
21. Indiana University Libraries, "Indiana University Libraries Privacy Policy," last updated February 1, 2012, https://policies.iu.edu/policies/lib-01-libraries-privacy/index.html.
22. Syracuse University Libraries, "Privacy Policy."
23. San Diego State University Library, "Freedom of Access and Privacy," https://library.sdsu.edu/about-us/policies-guidelines/freedom-access-privacy.
24. University of Miami Libraries, "Privacy Policy," https://www.library.miami.edu/about/privacy-policy.html.
25. University of Chicago Library, "Privacy Statement."
26. University of North Carolina at Chapel Hill Libraries, "Privacy Policy," last updated March 19, 2018, https://library.unc.edu/about/policies/privacy-policy/.
27. University of California Berkeley Library, "Collection, Use, and Disclosure of Electronic Information," last updated September 22, 2008, https://www.lib.berkeley.edu/about/privacy-electronic-information.
28. University of Michigan Library, "Library Privacy Statement."
29. Villanova University, Falvey Memorial Library, "Privacy Policy," last updated August 22, 2018, https://library.villanova.edu/using-the-library/access/privacy-policy.
30. University of Oregon Libraries, "UO Libraries Privacy Statement," last updated March 3, 2020, https://library.uoregon.edu/policies/privacystatement.
31. Auburn University Libraries, "Auburn University Libraries Privacy Policy," February 2006, https://www.lib.auburn.edu/policy/privacy_policy.pdf.
32. Atlanta-Fulton Public Library System, "Privacy Statement," http://afpls.org/privacy-statement.
33. Berkshire Athenaeum, "Website Policy; Computer Services Policy," 2010, https://static1.squarespace.com/static/5c7eed16e8ba44443d295e02/t/5cb17e6afa0d60178b15fcd3/1555136107037/BA_WebsitePolicy.pdf.
34. Lower Macungie Library, "E-Privacy Statement," Policies, https://www.lowermaclib.org/about-us/policies/.
35. Mount Prospect Public Library, "Online Terms of Use," https://mppl.org/wp-content/uploads/2011/08/Online-terms-of-use-0517.pdf.
36. Nashville Public Library, "Privacy Notice," last updated May 2, 2016, https://library.nashville.org/privacy-notice.
37. Ann Arbor District Library, "Ann Arbor District Library Privacy Statement Policy," last updated February 17, 2014, https://aadl.org/aboutus/policies/privacy.
38. Phoenix Public Library, "E-Privacy," June 16, 2010, https://www.phoenixpubliclibrary.org/AboutUs/Documents/Policies/E-Privacy.pdf.
39. Queens Borough Public Library, "Privacy Policy," December 2003, https://www.queenslibrary.org/about-us/library-policies/privacy.
40. Michigan State University Libraries, "Michigan State University Libraries Privacy Statement," https://lib.msu.edu/about/privacystmt/.
41. University of Oregon Libraries, "Privacy Statement."
42. Josephine-Louise Public Library, "Privacy Statement," https://www.waldenlibrary.org/privacy.aspx.
43. Pierce County Library System, "Website Privacy Policy," last updated October 11, 2007, https://www.piercecountylibrary.org/about-us/policies/website-privacy-policy.htm.
44. Los Angeles Public Library, "Online Privacy Policy," last updated March 2018, https://www.lapl.org/online-privacy-policy.
45. Penn State University Libraries, "Policy UL-AD08: Confidentiality and Privacy of Patron Library Records," last updated December 2017, https://libraries.psu.edu/policies/ul-ad08.
46. Harvard Library, "Harvard Library's Privacy Statement," Privacy, Terms of Use and Copyright Information, https://library.harvard.edu/privacy-terms-use-copyright-information#privacy.
47. Syracuse University Libraries, "Privacy Policy."
48. University of Denver Libraries, "Your Privacy and University Libraries," https://library.du.edu/policies/records-privacy.html.
49. Auburn University Libraries, "Privacy Policy."
50. University at Albany Libraries, "Internet Privacy Policy."
51. University of Chicago Library, "Privacy Statement."
52. University of Denver Libraries, "Your Privacy."
53. Pierce County Library System, "Website Privacy Policy."
54. Queens Borough Public Library, "Privacy Policy."
55. San José Public Library, "Privacy Policy," last updated March 12, 2018, https://www.sjpl.org/privacy-policy.
56. Duke University Libraries, "Privacy Statement."

57. Middlebury Library, "Privacy and Security of Library Records," https://www.middlebury.edu/library/about/policies/privacy-security.
58. Temple University Libraries, "Virtual Reference Privacy Guidelines," https://library.temple.edu/services/privacy.
59. Texas State University Libraries, "Virtual Reference Policy (Ask a Librarian @Alkek)," 2014, https://www.library.txstate.edu/about/policies/virtual-reference.htm.
60. Syracuse University Libraries, "Privacy Policy."
61. Syracuse University Libraries, "Privacy Policy."
62. University of North Carolina at Chapel Hill Libraries, "Privacy Policy."
63. Brown County Library, "Privacy and Confidentiality," May 15, 2014, https://www.browncountylibrary.org/wp-content/uploads/2012/09/H_1-Privacy-and-Confidentiality.pdf.
64. Josephine-Louise Public Library, "Privacy Statement."
65. Lower Macungie Library, "Patron/Donor Information Collection Policy," June 30, 2011, https://www.lowermaclib.org/wp-content/uploads/2014/09/Patron-Donor-Information-Collection-Policy-1.pdf.
66. Duke University Libraries, "Privacy Statement."
67. Montana State University Library, "Montana State University Privacy Policy," www.lib.montana.edu/privacy-policy/.
68. Texas Tech University Libraries, "Personally Identifiable Information," TTU Libraries' Privacy Policy, https://www.depts.ttu.edu/library/about/admin/privacy_policy.php.
69. Syracuse University Libraries, "Privacy Policy."
70. Fairbanks North Star Borough Public Libraries, "Borrowing Services," Policies and Procedures, last updated November 21, 2018, https://fnsblibrary.org/about/polpro/.
71. Geauga County Public Library, "Retention of Circulation Records," Geauga County Public Library Operating Policy Manual, December 17, 2019, http://divi.geaugalibrary.net/wp-content/uploads/2020/01/712-Retention-of-Records.pdf.
72. Las Vegas–Clark County Library District, "Patron Privacy Policy."
73. Cornell University Library, "Library Practices on the Collection, Use, Disclosure, Maintenance and Protection of Personally-Identifiable Information," https://www.library.cornell.edu/practices.
74. University of California San Diego Library, "Privacy Policy," last updated August 24, 2004, https://library.ucsd.edu/about/policies/privacy-policy.html.
75. Southern Illinois University Morris Library, "Patron Privacy Policy," December 2, 2015, https://lib.siu.edu/about/policies/patron-privacy-policy.php.
76. San Diego State University Library, "Freedom of Access and Privacy."
77. Rutgers University Libraries, "Privacy Policy."
78. Ann Arbor District Library, "Privacy Statement Policy."
79. Nashville Public Library, "Social Media and Blog Guidelines for Using, Commenting, and More," https://library.nashville.org/about/policies/social-media-and-blog-guidelines.
80. Berkshire Athenaeum, "Social Networking Policy; Computer Services Policy," 2010, https://static1.squarespace.com/static/5c7eed16e8ba44443d295e02/t/5cb17e4ae5e5f08d01334279/1555136074569/BA_SocialNetworkingPolicy.pdf.
81. Jessamine County Public Library, "Social Media Policy," last updated September 25, 2019, https://jesspublib.org/wp-content/uploads/3.5-Social-Media-Policy-2019-09-25.pdf.
82. Ann Arbor District Library, "Privacy Statement Policy."
83. Genesee District Library, "GDL Policy 5.9: Fundraising," *Policy Manual* (Flint, MI: Genesee District Library, 2016), https://www.thegdl.org/wp-content/uploads/Policies/Policy-Manual-for-Website.pdf.
84. Ocean County Library, "Camera Surveillance," Policies, Fees, and Forms, last updated April 19, 2016, https://theoceancountylibrary.org/policies-fees-forms.
85. Jessamine County Public Library, "Security Camera Policy," last updated August 18, 2010, https://jesspublib.org/wp-content/uploads/4.2-Security-Camera-Policy-2010-8-18.pdf.
86. Alpha Park Public Library District, "Security/Surveillance System Policy," Alpha Park Public Library District Policies, October 21, 2019, www.alphapark.org/images/webpolicies/securitysurveillancesystempolicy.pdf.
87. University of Oregon Libraries, "Security Cameras—Unit Level Policy," last updated June 20, 2016, https://library.uoregon.edu/policies/security_cameras.
88. University of North Carolina at Chapel Hill Libraries, "Privacy Policy."
89. Genesee District Library, "GDL Policy 4.7: Photography and Video Recording," *Policy Manual* (Flint, MI: Genesee District Library, 2016), https://www.thegdl.org/wp-content/uploads/Policies/Policy-Manual-for-Website.pdf.
90. St. Louis Public Library, "Photography, Filming and Videography Policy," 2013, https://www.slpl.org/service-policies/filming-and-photography-policy/.
91. University of Denver Libraries, "Your Privacy."
92. Ann Arbor District Library, "Privacy Statement Policy."

Chapter 4

Third-Party Platforms

Many libraries rely to some degree on applications hosted outside the library's direct administrative control or ownership, such as library services platforms, applications hosting and provisioning content (electronic journal publishers, e-book content providers, etc.), analytics tools, social media platforms, and more. Many services offer personalization features or other unique account-based services allowing end users to tailor their experience. Some services collect data that by itself could be considered private information; the potential also exists that data streams from one application could be combined with data from another application to create a more detailed profile of the user. In today's increasingly distributed environment, the library can no longer be considered the sole gatekeeper of its patrons' private information, emphasizing the present reality that data privacy can be confusing, ambiguous, and opaque.

ALA's Privacy Tool Kit and associated work demonstrate sound recognition of how distributed and complex today's online library environment has become. ALA's *Resolution on the Retention of Library Usage Records* urges, among other things, that libraries "assure that vendor agreements guarantee library control of all data and records."[1] The Tool Kit's "Developing or Revising a Library Privacy Policy" notes, "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."[2] Related to privacy concerns with emerging technologies, it notes, "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."[3] It further notes concerns with various types of applications and hosting models that have increasingly become the norm, such as apps, cloud computing, OPACs, and social networking tools.

ALA's "Privacy and Confidentiality Q&A" notes several related questions, for example,

> 22. Does the library's responsibility for user privacy and confidentiality extend to licenses and agreements with outside vendors and contractors?
>
> Most libraries conduct business with a variety of vendors in order to provide access to electronic resources, to acquire and run their automated systems, and in some instances, to offer remote storage (e.g. "cloud computing") or to enable access to the Internet. Libraries need to ensure that contracts and licenses reflect their policies and legal obligations concerning user privacy and confidentiality. Whenever a third party has access to personally identifiable information (PII), the agreements need to address appropriate restrictions on the use, aggregation, dissemination, and sale of that information, particularly information about minors. In circumstances in which there is a risk that PII may be disclosed, the library should warn its users.[4]

Similarly, *Privacy: An Interpretation of the Library Bill of Rights* notes,

> Libraries should never share users' personally identifiable information with third parties or vendors that provide resources and library services, unless the library obtains explicit permission from the user or if required by law or existing contract. Libraries or their governing institutions should negotiate agreements with vendors that retain library ownership of user data and permit independent auditing of vendor data collection, retention,

> and access policies and practices. Such agreements should stipulate that user data is confidential and that it may not be used or shared except with the permission of the library.[5]

As noted in chapter 1, ALA's Intellectual Freedom Committee has created several privacy checklists, many of which can apply to third-party vendor relationships where the application, service, or content is hosted outside the library's direct control and possession. These checklists provide guidance on recommended data stewardship related to vendors and steps the library can take to better inform its patrons about third-party privacy considerations and practices. As just one example, the "Library Privacy Checklist for E-Book Lending and Digital Content Vendors" notes,

> Provide links to vendor privacy policies and terms of service pages for users when appropriate, e.g. from the library's own privacy policy page or from a library web page about the vendor's product or service.
>
> Work with vendors to configure services to use the opt-in method whenever possible for features that involve the collection of personal information.
>
> . . .
>
> Add privacy considerations to the library's selection criteria for new purchases or the renewal of existing purchases.[6]

ALA's "Library Privacy Guidelines for Vendors" notes,

> Libraries and vendors must work together to ensure that the contracts and licenses governing the collection, processing, disclosure, and retention of library user data reflect library ethics, policies, and legal obligations concerning user privacy and confidentiality.
>
> . . .
>
> **Agreements, Ownership of User Data, and Legal Requirements**
>
> Agreements between libraries and vendors should address appropriate restrictions on the use, aggregation, retention, and disclosure of user data, particularly information about minors. Agreements between libraries and vendors should also specify that libraries retain ownership of all user data and that the vendor agrees to observe the library's privacy policies and data retention and security policies.
>
> . . .
>
> Privacy policies should be made readily accessible and understandable to users. Safeguarding user privacy requires that individuals know what information is gathered about them, how long it is stored, who has access to it and under what conditions, and how it is used. There should be a way to actively notify ongoing users of any changes to the vendor's privacy policies.
>
> . . .
>
> **Company Sale, Merger, or Bankruptcy:** In the event that a vendor is sold to another company, merges with another company, or is dissolved through bankruptcy, all personally identifiable information should be held under the same privacy policy or securely destroyed. Libraries and their users should be notified and provided a method to request that their data be securely destroyed or exported.[7]

In the library privacy policies examined, applications housed outside the libraries' direct administrative control were indeed often called "third-party" providers or websites; this occurred in seventeen of the academic library and fourteen of the public library policies analyzed. An additional ten libraries referred to such services but without the specific moniker "third-party." Other terminology used included "internet sites and services outside the administrative domain"[8] and "other sites and services that are not contained nor controlled within the Library's online environment."[9] This chapter will focus on several important considerations related to third parties, including how libraries typically do not share private patron information outside the library, how libraries working with vendors encourage them to adhere to the library's privacy practices, and how notices encourage patrons to review the policies of third-party vendors.

Sharing of Private Information

Many library policies explicitly indicate the libraries do not share customer information with outside entities (which could be third-party providers or other third parties that do not provide services or content to the library). Several verbs are used across the policies to denote that the library does not share information, including *sell, lend, license, disclose, provide, lease, rent, release, share, give, transfer, trade,* and *provide access*. Several policies indicate more generally that the library keeps information confidential and access is not provided for commercial use. At least half of the public library policies analyzed and fifteen of the

academic library policies made specific reference to how they do not share confidential information with third parties. As with other analysis points in this study, the fact that some policies don't specifically address the sharing of information with outside entities does not imply or suggest that the library does sell information to outside entities—only that sharing of information wasn't specifically referenced in the policy. For example, numerous policies indicate that confidential information will be released only by court order, and so on, and this implies that the library does not, for example, sell information for commercial use, even if the explicit reference does not appear. Several policies specifically note that their state's law explicitly prohibits any practice of selling information, such as Beaufort County Library's policy, which states, "Under Title 60-4-10 of the South Carolina Code of Laws, the Library may not sell, trade or rent its customers' personal information."[10] Examples of library policy phrasing stating that the library does not sell, lease, and so on confidential information follow.

East Greenbush Community Library

> The Library does not sell, lease, or otherwise distribute or disclose patron name, email address, postal address, telephone number, or other personal information to outside parties.[11]

Musser Public Library

> The library will hold confidential the names of card holders and their registration information, including email addresses, and not provide access for private, public or commercial use.[12]

Genesee District Library

> All gifts, grants, and/or support must ensure the confidentiality of user records. The library will not sell or provide access to library records in exchange for gifts or support.[13]

Phoenix Public Library

> Phoenix Public Library does not sell, rent, lease, or otherwise provide its customer lists or customer-controlled information to third parties.[14]

Cornell University Library

> The Library will not sell, share, or otherwise distribute your personal data to third parties without your consent.
>
> . . .
>
> The Library expects the information service providers with whom we contract to protect the identity of individual users and the information they use. We commonly require, for example, that vendors agree not to sell or license information from library users to third parties.[15]

Montana State University Library

> If you consent to give us your personally identifiable information, we will keep it confidential and will not sell, license, or disclose personal information to any third party without your consent, unless we are compelled to do so under the law or to comply with a court order.
>
> . . .
>
> Third Party Security: We ensure that our library's contracts, licenses, and off-site computer service arrangements reflect our policies and legal obligations concerning user privacy and confidentiality. Should a third party require access to our users' personally identifiable information, our agreements address appropriate restrictions on the use, aggregation, dissemination, and sale of that information.[16]

Cornell University Library's document "Library Practices on the Collection, Use, Disclosure, Maintenance and Protection of Personally-Identifiable Information" has a section titled "Licensed Service Case Study: The Library Catalog," wherein the library describes its use of OCLC's services for its library catalog, references OCLC's service terms and conditions, and provides some analysis of the types of information collected as well as the fact that "individual users are not connected to activities performed on the site. . . . Searches conducted and records viewed cannot be tied back to individual users."[17]

Working with Vendors to Respect Library Privacy Policies and Values

Several professional organizational statements or frameworks have been developed to encourage vendor respect for library privacy practices. The International Coalition of Library Consortia's *Privacy Guidelines for Electronic Resources Vendors* advocates that vendors draft transparent and accessible privacy policies that empower and protect end users and seeks adherence to the ALA *Code of Ethics*.[18] Harvard Library's privacy policy references this document: "Our commitment to user privacy extends to our agreements with online content providers, including support for the International Coalition of Library

Consortia (ICOLC) Privacy Guidelines for Electronic Resources Vendors."[19]

Stanford Libraries' "Statement on Patron Privacy and Database Access" states that providers increasingly have data-gathering practices in conflict with a library patron's right to privacy and notes, "It is important for libraries to monitor these developments and redirect them in favor of patron privacy in order to safeguard our role as trusted providers in the information age."[20] Duke University Library's privacy policy references the Stanford Libraries' statement: "DUL additionally endorses the Stanford Libraries Statement on Patron Privacy and Database Access."[21]

Approximately fifteen academic library and three public library policies provided some reference noting their libraries' efforts seeking to ensure that commercial vendors adhere to the local library's privacy stance.

Encouraging Patrons to Review the Policies of Third-Party Vendors

Approximately twenty-seven of the academic library and twenty-four of the public library policies make some reference to third-party privacy policies and the ways those vendor policies apply when patrons are using that site or service, encouraging patrons to read the privacy policies of third-party vendors. Phrasing varies broadly, but a core, cautionary, and underlying message is that providers have their own policies, that the patron is subject to those policies, and that third parties may not value patrons' privacy to the same degree as the library.

Brown County Library

> The Library does not collect information about who library users are, but other organizations might. The Library encourages library users to become familiar with the privacy policies of their ISP (Internet Service Provider) and the websites that they visit to learn what information might be collected elsewhere online.
>
> . . .
>
> The Library's website contains links to other sites. The Brown County Library is not responsible for the privacy practices of other sites, including providers of online database services for which the Library subscribes, which may be different from the privacy practices described in this policy. The Library encourages library users to become familiar with privacy policies of other sites visited, including linked sites.[22]

Nashville Public Library

> You are agreeing to be bound by these terms, all applicable laws and regulations, and any other applicable policies, terms and guidelines established by NPL and those of any third parties that host our sites (such as Facebook or Twitter).[23]
>
> Nashville Public Library's website includes many links to outside sources. Those sites have different privacy statements and the Library's notice does not apply. Individuals should always take care before sharing personal information, credit card numbers, or other sensitive information via the Internet.[24]

Los Angeles Public Library

> Depending on the third-party tool's business practices, privacy policies, terms of service, and/or the privacy settings you selected, the information you have provided to third parties could be used to identify you when you visit lapl.org. These third parties do not/will not share your identity with lapl.org.
>
> . . .
>
> Non-library websites may be linked through the library's website. Many non-library sites may or may not be subject to the Public Records Act and may or may not be subject to other sections of California Code or federal law. Visitors to such sites are advised to check the privacy statements of such sites and to be cautious about providing personally identifiable information without a clear understanding of how the information will be used.[25]

Rutgers University Libraries

> Third Party Security: The Rutgers University Libraries use and link to resources owned and operated by third parties, including integrated library systems, offsite computer services, databases, and electronic journals. We license these resources for the use of Rutgers authorized users. We make every attempt to include user privacy protections in license agreements with third parties, such as vendors of digital information resources like electronic databases and journals. Nevertheless, because the use of these websites and resources is not governed by the Rutgers University Libraries, we strongly recommend that you review the privacy policies of the websites that you visit, particularly if you are requesting online help through email or chat or establishing your own account for

specialized services like table of contents, email, saved search alerts, purchases, or personalization features. When connecting to licensed resources outside the library, we authenticate users as members of our community and do not provide any personally identifiable information.[26]

University of North Carolina at Chapel Hill Libraries

Vendors and Other Entities

On The University of North Carolina at Chapel Hill Libraries' behalf, vendors and other third parties may provide certain services available on the libraries' Web sites. The University of North Carolina at Chapel Hill Libraries may provide information, including personal information, collected on the Web to third-party service providers to help us deliver programs, products, information and services. Service providers are also an important means by which The University of North Carolina at Chapel Hill Libraries maintains its Web site and mailing lists. We will take reasonable steps to ensure that these third-party service providers are obligated to protect, de-identify, or dispose of personal information on our behalf.

We license resources from vendors who may, in turn, request information from you for services, e.g., "notify me" or "alert" services. We encourage you to understand the privacy policies of those vendors and take personal responsibility for protecting your personal information.[27]

Utah State University Libraries

USU Libraries website may contain links to other resources that are independently managed. The Library also contains links to sources outside the university. These sites may have their own privacy policy or may have none at all. We urge you to use caution when providing personal information to any of these websites.[28]

Cornell University Library

More and more, the Library outsources systems and services to third-party vendors. Most of the digital resources that we offer, for example, come from outside suppliers, as does the current Library Catalog. The Library expects the information service providers with whom we contract to protect the identity of individual users and the information they use. We commonly require, for example, that vendors agree not to sell or license information from library users to third parties. Many vendors provide additional personalized services that may require you to identify yourself with your name or a pseudonym. In general, this is done at your discretion; the Library seeks to avoid products that demand personalization.

While the Library seeks to require third parties with which it works to follow accepted library policies regarding privacy and confidentiality, it is not responsible for the privacy practices of these third parties. We encourage users to familiarize themselves with third party privacy policies before using the resources.[29]

Google Analytics

Google Analytics appeared to be the single most referenced third-party platform across the analyzed policies, mentioned by name in at least nine of the public and thirteen of the academic library policies, and its use seems implied in the policies of several additional libraries. Some policies go into greater detail about their use of Google Analytics, for example, the University of California Berkeley Library's policy:

Google Analytics

The UC Berkeley Library uses Google Analytics to capture and analyze web statistics. Google Analytics is a cookie-based analytics program that uses cookies to track website activity. Google Analytics typically collects, at least temporarily, the following information: Network Location; Hostname; web pages requested; referring web page; browser used; screen resolution; date and time. No personal information is stored within cookies. Cookies can be disabled within a browser's preference or option menu.

For more information about Google Analytics, see Google Privacy Center—Privacy Policy.[30]

Several policies note that the user can curtail the information collected, for example, the University of Denver Libraries' policy:

The Libraries' website (OmniUpdate), research guides (Springshare), A-Z database list, Special Collections @ DU, Archives @ DU (Archives Space), Digital Commons @ DU (Digital Commons), Compass (Primo), Online Exhibits (Omeka), and Yewno are tracked using Google Analytics. Data gathered include the browser, operating system, and city of the device being used, searches performed, and site navigation. The Libraries do not use Google Advertising Features, so no personal or demographic data are made available to the Libraries

via Analytics. However, if you are logged into your Google Account while using the Libraries' website or tools, additional data may be tracked and linked to your Google Account.

Additional information, including instructions on adjusting what data Google connects to your account, can be found at:

https://myaccount.google.com/privacy.

Google also offers a browser add-on that allows you to opt out of Google Analytics:

https://tools.google.com/dlpage/gaoptout.[31]

The University of Michigan Library's policy provides three alternatives on how one can opt out of Google tracking.[32]

Notes

1. American Library Association, *Resolution on the Retention of Library Usage Records* (Chicago: American Library Association, 2006), 1, https://alair.ala.org/bitstream/handle/11213/1594/52.4.4%20Retention%20of%20Library%20Records.pdf.
2. American Library Association, "Developing or Revising a Library Privacy Policy," Privacy Tool Kit, last updated April 2017, www.ala.org/advocacy/privacy/toolkit/policy.
3. American Library Association, "Developing or Revising."
4. American Library Association, "Privacy and Confidentiality Q&A," last updated July 29, 2019, www.ala.org/advocacy/intfreedom/privacyconfidentialityqa.
5. American Library Association, *Privacy: An Interpretation of the Library Bill of Rights* (Chicago: American Library Association, 2002, amended 2014, 2019), www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy.
6. American Library Association, "Library Privacy Checklist for E-Book Lending and Digital Content Vendors," last updated January 26, 2020, www.ala.org/advocacy/privacy/checklists/ebook-digital-content.
7. American Library Association, "Library Privacy Guidelines for Vendors," last updated January 26, 2020, www.ala.org/advocacy/privacy/guidelines/vendors.
8. University of Miami Libraries, "Privacy Policy," https://www.library.miami.edu/about/privacy-policy.html.
9. University of California Los Angeles Library, "Privacy Policy," https://www.library.ucla.edu/use/access-privileges/privacy-policy.
10. Beaufort County Library, "Website User Agreement," 2009, https://2f26905f-7709-4fc5-8602-f82d730cafe1.filesusr.com/ugd/a57334_001fd0492b624dd386bc22e42903daf2.pdf.
11. East Greenbush Community Library, "Privacy Policy," https://eglibrary.org/about/policies/#privacy.
12. Musser Public Library, "Confidentiality Policy," August 19, 2015, https://musserpubliclibrary.org/wp-content/uploads/2018/08/Confidentiality-Policy.pdf.
13. Genesee District Library, "GDL Policy 5.5: Donations, Grants and Monetary Gifts," *Policy Manual* (Flint, MI: Genesee District Library, 2016), https://www.thegdl.org/wp-content/uploads/Policies/Policy-Manual-for-Website.pdf.
14. Phoenix Public Library, "E-Privacy," June 15, 2010, https://www.phoenixpubliclibrary.org/AboutUs/Documents/Policies/E-Privacy.pdf.
15. Cornell University Library, "Library Practices on the Collection, Use, Disclosure, Maintenance and Protection of Personally-Identifiable Information," https://www.library.cornell.edu/practices.
16. Montana State University Library, "Montana State University Privacy Policy," www.lib.montana.edu/privacy-policy/.
17. Cornell University Library, "Library Practices."
18. International Coalition of Library Consortia, *Privacy Guidelines for Electronic Resources Vendors* (International Coalition of Library Consortia, 2002), https://icolc.net/statement/privacy-guidelines-electronic-resources-vendors; American Library Association, *Code of Ethics of the American Library Association* (Chicago: American Library Association, 1939, amended 1981, 1995, 2008), www.ala.org/advocacy/sites/ala.org.advocacy/files/content/proethics/codeofethics/Code%20of%20Ethics%20of%20the%20American%20Library%20Association.pdf.
19. Harvard Library, "Harvard Library's Privacy Statement," Privacy, Terms of Use and Copyright Information, https://library.harvard.edu/privacy-terms-use-copyright-information#privacy.
20. Stanford Libraries, "Statement on Patron Privacy and Database Access," https://library.stanford.edu/using/special-policies/statement-patron-privacy-and-database-access.
21. Duke University Libraries, "Duke University Libraries Privacy Statement," https://library.duke.edu/about/privacy.
22. Brown County Library, "Privacy and Confidentiality," May 15, 2014, https://www.browncountylibrary.org/wp-content/uploads/2012/09/H_1-Privacy-and-Confidentiality.pdf.
23. Nashville Public Library, "Social Media and Blog Guidelines for Using, Commenting, and More," https://library.nashville.org/about/policies/social-media-and-blog-guidelines.
24. Nashville Public Library, "Privacy Notice," last updated May 2, 2016, https://library.nashville.org/privacy-notice.
25. Los Angeles Public Library, "Online Privacy Policy," last updated March 2018, https://www.lapl.org/online-privacy-policy.
26. Rutgers University Libraries, "Privacy Policy," October 19, 2010, https://www.libraries.rutgers.edu/privacy_policy.
27. University of North Carolina at Chapel Hill Libraries, "Privacy Policy," last updated March 19, 2018, https://library.unc.edu/about/policies/privacy-policy/.
28. Utah State University Libraries, "Utah State University Libraries Privacy Statement," https://arwen.lib.usu.edu/privacy_policy/.

29. Cornell University Library, “Library Practices.”
30. University of California Berkeley Library, “Collection, Use, and Disclosure of Electronic Information,” last updated September 22, 2008, https://www.lib.berkeley.edu/about/privacy-electronic-information.
31. University of Denver Libraries, “Your Privacy and University Libraries,” https://library.du.edu/policies/records-privacy.html.
32. University of Michigan Library, “Library Privacy Statement,” last updated March 2016, https://www.lib.umich.edu/library-administration/library-privacy-statement.

Chapter 5

Data Security, Integrity, and Retention

What data is collected and how libraries use such data—the topic of preceding chapters—is important. So, too, are the protections related to—and ultimate disposition of—data that is collected. This chapter focuses on data security and integrity and on the ultimate disposition of that data (data retention practices). To begin, the analyzed policies provide varying levels of detail regarding their libraries' data integrity and security practices. ALA's Privacy Tool Kit section "Developing or Revising a Library Privacy Policy" notes the following, and this verbiage appears in several of the library policies analyzed:

> **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.[1]

The ALA guidance also includes recommendations regarding data security (including administrative measures):

> **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.[2]

Discussion of data integrity and security practices did not appear to be a major focus for many policies. Several library policies directly and honestly note the challenges of safeguarding data. Southern Illinois University Morris Library's policy notes, "Although no method can guarantee the complete security of data, we take steps to protect the privacy and accuracy of patron data."[3] The University of California San Diego Library's policy notes,

> To guard against unauthorized access, maintain data accuracy, and promote the correct use of information, we have implemented physical,

electronic, and managerial procedures to safeguard and secure the information we collect online.

However, while we consider these measures reasonable, no guarantee can be given that they will always prevent or protect against invalid access or improper activity. For this reason, we avoid keeping information beyond the term of its primary use and, where possible, encrypt or delete data elements that might cause activities to be linked to individual users.[4]

The University of Chicago Library's privacy policy notes, "While the Library makes a concerted effort to protect personal information, we cannot guarantee that your submissions to our website, any content residing on our servers, or any transmissions from our server will be completely secure."[5]

In a different light, an ancillary document to the University of California Berkeley Library's policy notes the possibility of unintentional observation of data:

> **Unavoidable Inspection.** During the performance of their duties, personnel who operate and support electronic communications resources periodically need to monitor transmissions or observe certain transactional information to ensure the proper functioning and security of Library systems and services. On these and other occasions, systems personnel might observe personally identifiable information. Except as provided elsewhere in this Policy or by law, they are not permitted to seek out such information where not germane to the foregoing purposes, or disclose or otherwise use what they have observed.[6]

Numerous public library policies (much more frequently than academic library policies) reference the challenging security associated with Wi-Fi networks. For example, the St. Louis Public Library's "Library Technology Acceptable Use Policy" notes,

> Users should be aware that the Internet is not a secure medium and that third parties may be able to obtain information regarding users' activities. . . .
>
> Users should understand and acknowledge that Hotspots are unsecured, wireless networks and that any information being sent or received over the network could potentially be intercepted by another wireless user. Users are cautioned against transmitting their credit card information, passwords, and any other sensitive, personal information while using the wireless network.[7]

Other policies note care should be taken with configuration of personal devices, such as Las Vegas–Clark County Library District's "Internet and Wireless Use Policy":

> **Use of Personal Equipment**
>
> . . .
>
> In light of security issues and the variety of equipment that can be used to access wireless networks, the District urges patrons to incorporate appropriate protections systems such as anti-virus, firewall software and updated patches when accessing the District's wireless network. The District does not provide encryption services and does not guarantee privacy of data transmitted across its network.[8]

Retention of Data

Often associated with the collection of data is the retention of data, as together they comprise the data life cycle. ALA's *Resolution on the Retention of Library Usage Records* notes,

> Dispose of library usage records containing personally identifiable information unless they are needed for the efficient and lawful operation of the library, including, but not limited to, data-related logs, digital records, vendor-collected data, and system backups. . . .
>
> The American Library Association urges members of the library community to advocate that records retention laws and regulations limit retention of library usage records containing personally identifiable information to the time needed for efficient operation of the library.[9]

The Privacy Tool Kit's section "Developing or Revising a Library Privacy Policy" notes,

> **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.[10]

Some of the analyzed policies provided broad, generalized references to length of data retention, with phrasings such as "regularly remove," as opposed to

something more specific, such as "each week." Some policies provide additional, more detailed retention information on one or more particular data types. Examples of broad, generalized data retention references follow (and note some of the policies below provide more specific retention details later in their policies):

Indiana University Libraries

> In all cases involving personally identifiable information, it is our policy to . . . avoid retaining records not needed for the fulfillment of the mission of the library.
>
> . . .
>
> Our goal is to collect and retain only the information we need to provide library-related services.
>
> . . .
>
> *Data Integrity:* We take reasonable steps to assure data integrity, including . . . destroying untimely data or converting it to anonymous form.
>
> *Data Retention:* We regularly review and purge personally identifiable information once it is no longer needed to manage library services. Information that is regularly reviewed for purging includes, but is not limited to, personally identifiable information on library resource use, material circulation history, and security/surveillance tapes and logs.
>
> . . .
>
> The IU Libraries follow University policy for the retention of data. . . .
>
> Data about which users were connected to which machine is collected, in accordance with University policy, and kept for a limited time with very limited access by staff.
>
> . . .
>
> We regularly remove cookies, web history, cached files, and other use records from library computers and networks.[11]

University of Michigan Library

> **How long will you keep data about the use of Library services?**
>
> It depends on the data and how we are using it. Some data will be kept indefinitely, other data is stored and used for shorter periods. We only keep data as long as it is useful for the services we provide.[12]

University of Chicago Library

> Identifiable information may be retained, in some cases indefinitely, when doing so serves an institutional purpose.[13]

University of California San Diego Library

> Where it is necessary for the Library to identify users, it is our goal to gather only the minimum information necessary and to retain that information for only as long as it is needed to complete a particular transaction.
>
> . . .
>
> **Site Security**
>
> We avoid keeping information beyond the term of its primary use and, where possible, encrypt or delete data elements that might cause activities to be linked to individual users.[14]

Mount Prospect Public Library

> The Library will make all practicable efforts to retain records containing patron-identifiable information only to the extent necessary to preserve Library or public property or to fulfill another core library function.[15]

Pierce County Library System

> Library records containing personally identifiable information will be disposed of unless needed for efficient operation of the library, public records retention requirements, system backups, or other reasons related to effectively managing library resources or providing services.[16]

Las Vegas–Clark County Library District

> In accordance with NRS 239, the District will not retain any records pertaining to a patron's use of library resources longer than necessary to provide appropriate stewardship of those resources.
>
> . . .
>
> *Data Retention:* The District protects personally identifiable information from unauthorized disclosure once it is no longer needed to manage library services. Information that should be regularly

> purged or shredded includes personally identifiable information on library resource use, material circulation history, and security/surveillance tapes and logs.[17]

ALA's "Library Privacy Checklist—Overview" (as well as the checklists associated with specific systems) provides additional retention guidance on particular data types, for example, circulation transaction data: "Purge circulation and interlibrary loan records when they are no longer needed for library operations. Any patron data that is kept for analysis should be anonymized or de-identified and have access restricted to authorized staff."[18]

Indeed, across the analyzed policies, one of the most frequent retention-related references to a specific data type is circulation data. In many but not all instances, it's noted that upon the return of an item to the library, the information tying the patron to that item is erased. Many policies note exceptions related to instances in which a fine or fee is accrued or in which a user has opted for the system to maintain a list of past items checked out. Library policies can provide more time frame–specific information on one or more data types, such as

- circulation data
- interlibrary loan and document delivery data
- end user computer and resource use data
- reference transaction data
- video surveillance data
- patron record data
- social media and shared content data
- various types of computer use and network-related data, whether on a client or server computer

Circulation Data

Cornell University Library

> The Library seeks to protect user privacy by purging borrowing records as soon as possible. In general, the link connecting a patron with a borrowed item is broken once the item is returned. The exception is when a bill for the item is generated. In that case, the information on who borrowed the item is retained indefinitely in our system.[19]

Utah State University Libraries

> To safeguard patron information once a book is returned to the library the link between a patron and the item checked out is deleted. The only exception to this deletion is for books with fines or those books regarded as "lost" on a patron's account.[20]

University of Utah J. Willard Marriot Library

> The Library purges from its system all circulation records 30 days after a circulation transaction has closed and the items have been returned.[21]

University of Texas Libraries

> When a borrower returns materials to the library, if no fines or fees are assessed, information about the materials checked out is deleted from the library's online records twice monthly.[22]

Temple University Libraries

> The records of most circulation borrowing transactions are expunged and overwritten immediately upon return to the libraries of the loaned items and thereafter are reflected only as anonymized statistics descriptive of overall borrowing patterns.[23]

Southern Illinois University Morris Library

> Morris Library maintains records of circulation transactions only until the borrowed items are returned. Fines accrued for lost or overdue books are kept for record keeping purposes and only until the patron's record is purged. The library does not maintain histories of patrons' previously borrowed items.[24]

San Diego State University Library

> The Library will not track identifiable patron search history and will keep no record of such. The exceptions to this are:
>
> 1. In circumstances where format of material requires extensive time to verify the return of all relevant borrowed items (ie: a box containing dozens of documents etc). After full verification the patron data will not be kept except in the cases of rare and valuable materials where usage data may be kept indefinitely.[25]

University of Denver Libraries

> WHEN YOU CHECK OUT PRINT MATERIALS:
>
> . . .
>
> Once you return an item, and you do not owe a fine on the item, your checkout of the item is anonymized and the item cannot be traced back to you.[26]

East Greenbush Community Library

> Items that have been returned are automatically erased from a patron's record, unless they have opted to save their checkout history.[27]

Fairbanks North Star Borough Public Libraries

> The library does not maintain records of items that individuals have borrowed and returned in the past, except when there are unresolved issues with those items.[28]

Geauga County Public Library

> Circulation records and other records identifying the names of library users with specific materials are retained while the materials are charged to a patron and when materials are returned until of no further administrative value. The current ILS system retains patron information on items until the item is checked out to another patron.
>
> If an item is returned damaged and the fees are not paid, the library will retain the record until the matter is resolved.[29]

Queens Borough Public Library

> At the moment that library material is returned to the library, the link between the customer and the material is broken—the Library's system does not retain information on what materials were taken out by whom the moment the item is returned.[30]

Brown County Library

> The Library does not maintain a history of what a library user has previously checked out once books and materials have been returned on time. When fines accrue on a user's account, the Library does maintain records of items that have been borrowed but returned after the due date, or are still outstanding on the user's record.[31]

Jessamine County Public Library

> Personal data is privatized, i.e. made anonymous, in the Library's computer system so that log files cannot identify personal checkout history beyond 60 days.[32]

Las Vegas–Clark County Public Library

> District records that link a patron's identity to the use of library materials will be expunged upon the return in good standing of loaned materials to the District.[33]

San José Public Library

> The library does not keep a record of your reading history beyond operational requirements. Once you return an item it is removed from your account.[34]

Interlibrary Loan and Document Delivery Data

San Diego State University Library

> Information on materials received through Interlibrary Loan (ILL) are [*sic*] kept for one year.[35]

Berkshire Athenaeum

> The Athenaeum tracks interlibrary loaned items currently being borrowed and generates a paper record with patron information. After a period of six months, once the materials are returned to the owning library and all appropriate fines and/or fees are paid by the borrower, the paper trail record is destroyed.[36]

End User Computer and Resource Use Data

Cornell University Library

> Raw log files are normally maintained for 90 days for security purposes. . . . For some sites, an aggregated abstract of the data is prepared each night that anonymizes session data so that searches cannot be linked to specific IP addresses or network IDs.[37]

Harvard Library

> Data gathered about each session varies according to the method of connection to the resource. The resulting logs contain information necessary for analyzing the use of resources, troubleshooting problems and improving services.
>
> Log data is also used to distribute resource costs among Harvard libraries and faculties. These logs remain intact for approximately one fiscal year.[38]

University of Texas Libraries

> The University of Texas Libraries keeps the minimum number of records necessary to maintain operations. For example, when a user logs off a library computer, the library does not retain information that connects the user to activities performed during the session.[39]

University at Albany Libraries

> **Retention of Information Collected through This Web Site**
>
> In general, the Internet services logs of the University Libraries, comprising electronic files or automated logs created to monitor access and use of Agency services provided through this Web site, are retained for 60 business days and then destroyed. Occasionally, logs are retained longer for troubleshooting purposes. Information concerning these records retention and disposition schedules may be obtained through the Internet privacy policy contact listed in this policy.[40]

Southern Illinois University Morris Library

> Cookies, web history, and cached files are removed when a user closes a browser or logs off a machine.[41]

Rutgers University Libraries

> We remove cookies, web history, cached files, or other computer and Internet use records and other software code that is placed on our public computers or networks after each use.[42]

Warrenville Public Library District

> Public Access Computers
>
> The Warrenville Public Library District attempts to maintain strict security on public access computers to prevent any personal information from being retained after a workstation has been rebooted.[43]

Berkshire Athenaeum

> Once a search has been conducted, the software does not retain a copy of the search, and any records of the search will not exist.
>
> . . .
>
> The reservation management program retains patron identification information for only the current day's transactions. After the end of the business day, session information and statistical summary information can be generated; but patron identifying information is unavailable.
>
> Printouts from the library's public internet workstations are managed with an automated print management program. The program confirms print requests and alerts patrons and staff of print charges accrued. After a pending print job is released by staff for print out no record of the job remains.
>
> The security on the workstations wipes out the cache and/or history files each time a new computer session is started.
>
> . . .
>
> The search history of each PAC [catalog only station] is automatically erased every twenty-four hours.[44]

Ocean County Library

> When a computer session is ended, all information about that session is ordinarily deleted. At the end of the business day, all computer use and reservation records are normally erased.[45]

Durham County Library

> To use one of our public computers, you log on using your library card number. We do not keep a record of your activities during your session, such as browsing history, cookies, bookmarks, or downloads. The session data is automatically deleted from the computer after you log out. We do, however, keep a record of the fact that you logged on to that computer.[46]

Tampa-Hillsborough Public Library

> In accordance with this law [Florida Statutes Chapter 257.261], computer sign-in sheets are shredded as soon as all customers listed have been served or at the end of the day, whichever occurs first.
>
> . . .
>
> A library branch may choose to keep a daily log of guest pass distribution. . . . Sign-in sheets are to be shredded as soon as they are full or at the end of each day, whichever occurs first.[47]

San José Public Library

> The library does not keep a record of your activities on any public computer or laptop. Any record of browsing history and activities are [*sic*] removed when you log out.
>
> All personally identifiable information is purged immediately upon the end of your public computer reservation. An anonymous log is created that

includes only the computer terminal number, reservation time, and duration of the session. These anonymous reservation statistics remain in the system for two months.

All connected devices you borrow from the library (e.g. tablets, eReaders) have their history manually cleared by library staff immediately after you return the device.[48]

Reference Transaction Data

Texas State University Libraries

User Privacy

- The Alkek Library Ask a Librarian service records all reference transactions, including the chat conversation and the URLs for all the web sites visited.
- At the end of the session, you have the option to have the transcript emailed to you and a copy will be stored in our database for a period of one year.[49]

Temple University Libraries

Any patron may request to have their chat, email, or text transcript deleted by contacting the Libraries' Learning and Research Services department.[50]

Southern Illinois University Morris Library

In the case of email reference questions, we retain any personal information provided by the patron, such as name, email, phone number, until the question is resolved.[51]

Brown County Library

The Library treats reference questions, regardless of format of transmission (in person, via telephone, fax, email or online) confidentially. Identifying information related to these questions is purged on a minimum of two weeks.[52]

Video Surveillance Data

Berkshire Athenaeum

Video Surveillance: . . . Recorded images are saved for a period of eight weeks, at which point the storage medium is re-recorded.[53]

Western Plains Library System

Recordings from the WPLS video security system are stored digitally on restricted hardware at the Main Office and retained up to a minimum of 28 days. . . . Video records of incidents can be retained and reviewed as long as considered necessary by the Executive Director.[54]

Deer Park Public Library

Length of time recorded images are retained varies based on the storage capacity of the system hard drive.[55]

Mount Prospect Public Library

No video will be stored for more than the rolling window when the system overwrites the oldest video while recording the present.

. . .

The Library will retain specific footage of an incident until no longer needed. Video files will be reviewed annually by the Executive Director and the Director of Facilities and Security to decide whether to continue to retain or to dispose.[56]

Ocean County Library

Recorded information from security cameras is retained for one month, unless an incident occurs that requires holding the tape longer. . . .

Recorded information that is subpoenaed will be retained for one year.[57]

Las Vegas–Clark County Library District

Recordings from security cameras are stored no longer than 10 days, unless an incident occurs that requires holding the entire recording or a portion of the recording longer.[58]

Patron Record Data

Jessamine County Public Library

When a customer record is inactive for four (4) years and carries no outstanding debt (financial or in borrowed materials), the record is deleted from the Library's computer system and is not archived.[59]

Brown County Library

> **Library Cards and Circulation Records**
>
> To receive a library card, library users are required to provide identifying information such as name, birth date and mailing address. This identifying information is retained as long as the library user continues to use the library card.[60]

Pinellas Public Library Cooperative

> Cardholder accounts will be purged after 5 years of inactivity unless there are billed item fees on the account. All accounts, including delinquent accounts with billed item or collection referral fees, will be purged after 7 years of inactivity. Libraries follow the Florida Department of State's *General Records Schedule for Public Libraries* when reviewing records eligible for purging.[61]

Durham County Library

> For most cardholders, your account remains in the system as long as it is active. An account becomes inactive when it hasn't been used in three years and there are no outstanding fines or fees attached. At that point, it is deleted from our system. A few card types, such as non-resident cards, expire sooner—see our Registration Policy for details.[62]

Social Media and Shared Content Data

Nashville Public Library

> **The Library Is Bound by Records Retention Rules**
>
> What this means: A record of your usage and content will likely exist.
>
> All designated Metro government social media accounts shall follow archive guidelines set forth by the Public Records Commission.[63]

St. Louis Public Library

> Think before you post. You are legally liable for everything you post. Remember that the internet never forgets. Everything you post may be visible to the world even after you attempt to delete it.
>
> The content of the Library's social media is subject to public record laws, including the Missouri Sunshine laws. Relevant record retention schedules apply to social media content. Content must be managed, stored, and retrieved to comply with open records laws and e-discovery laws and policies.[64]

Hillsborough County Public Library Cooperative

> Moderators will maintain an archive containing all social media posts and comments in accordance with the State of Florida's General Records Schedule GS15 for Public Libraries.[65]

Parent Institution or System-wide Retention Schedules

Several library policies make reference to—and in some cases provide a link for—a different, higher-level record retention schedule or policy, such as a university schedule or a county government schedule.

University of Connecticut Library

> Library patron records are retained in accordance with the state record retention requirements established by the Office of the Public Records Administrator of the Connecticut State Library.[66]

University of California San Diego Library

> The Library's Billing Department retains all paper and electronic documents pertaining to and relevant for the collection of overdue fines, replacement charges, damaged-book fines/charges, and associated processing fees, according to the University of California Records Disposition Schedules Manual.[67]

Syracuse University Libraries

> The Libraries retain Individual Information associated with Business Transactions for a period of time mandated by state or federal tax laws, and consistent with the University's data retention schedule.[68]

Temple University Libraries

> At all times PII is to be secured in accordance with University policies and for limited time periods defined by record retention schedules.
>
> . . .
>
> Records containing PII which are scheduled for destruction shall be disposed of in accordance with University information security procedures.[69]

Cherokee Regional Library System

> The Cherokee Regional Library System shall follow the Local Government Records Retention Schedules for Local Government Paper and Electronic Records as set forth by the Georgia Secretary of State's Division of Archives and History.[70]

Genesee District Library

> **Records Retention**
>
> In order to meet the administrative, legal, fiscal, and archival requirements of the State of Michigan, the Genesee District Library will manage its records in accordance with the General Schedule #17 (GS #17) developed for Michigan public libraries.[71]

San José Public Library

> The library strives to collect the least amount of personally identifiable information we can. We avoid creating unnecessary records. We keep your information as long as required by the City of San José's Records Retention Schedule.[72]

Notes

1. American Library Association, "Developing or Revising a Library Privacy Policy," Privacy Tool Kit, last updated April 2017, www.ala.org/advocacy/privacy/toolkit/policy.
2. American Library Association, "Developing or Revising."
3. Southern Illinois University Morris Library, "Patron Privacy Policy," December 2, 2015, https://lib.siu.edu/about/policies/patron-privacy-policy.php.
4. University of California San Diego Library, "Privacy Policy," last updated August 24, 2004, https://library.ucsd.edu/about/policies/privacy-policy.html.
5. University of Chicago Library, "Privacy Statement," https://www.lib.uchicago.edu/about/thelibrary/policies/privacy/.
6. University of California Berkeley Library, "Collection, Use, and Disclosure of Electronic Information," last updated September 22, 2008, https://www.lib.berkeley.edu/about/privacy-electronic-information.
7. St. Louis Public Library, "Library Technology Acceptable Use Policy," last updated February 8, 2018, https://www.slpl.org/service-policies/technology/.
8. Las Vegas–Clark County Library District, "Internet and Wireless Use Policy," https://lvccld.org/wp-content/uploads/sites/54/2017/11/internet_wireless_use_policy.pdf.
9. American Library Association, *Resolution on the Retention of Library Usage Records* (Chicago: American Library Association, 2006), https://alair.ala.org/bitstream/handle/11213/1594/52.4.4%20Retention%20of%20Library%20Records.pdf.
10. American Library Association, "Developing or Revising."
11. Indiana University Libraries, "Indiana University Libraries Privacy Policy," last updated February 1, 2012, https://policies.iu.edu/policies/lib-01-libraries-privacy/index.html.
12. University of Michigan Library, "Library Privacy Statement—Frequently Asked Questions (FAQ)," last updated June 14, 2018, https://www.lib.umich.edu/library-administration/library-privacy-statement-frequently-asked-questions-faq.
13. University of Chicago Library, "Privacy Statement."
14. University of California San Diego Library, "Privacy Policy."
15. Mount Prospect Public Library, "Record Keeping Policy," https://mppl.org/wp-content/uploads/2018/07/Record-Keeping-Policy-0718.pdf.
16. Pierce County Library System, "Confidentiality of Library Records and Customer Files," last updated October 15, 2013, https://www.piercecountylibrary.org/about-us/policies/confidentiality-library-records.htm.
17. Las Vegas–Clark County Library District, "Patron Privacy Policy," last updated April 10, 2014, https://lvccld.org/wp-content/uploads/sites/54/2017/10/privacypolicy.pdf.
18. American Library Association, "Library Privacy Checklist—Overview," last updated January 26, 2020, www.ala.org/advocacy/privacy/checklists/overview.
19. Cornell University Library, "Library Practices on the Collection, Use, Disclosure, Maintenance and Protection of Personally-Identifiable Information," https://www.library.cornell.edu/practices.
20. Utah State University Libraries, "Utah State University Libraries Privacy Statement," https://arwen.lib.usu.edu/privacy_policy/.
21. University of Utah, J. Willard Marriott Library, "Privacy Policy," https://lib.utah.edu/pdf/Privacy_Policy_Procedures.pdf.
22. University of Texas Libraries, "Privacy and Confidentiality of Library Records Policy," https://www.lib.utexas.edu/about/policies/privacy-and-confidentiality-library-records-policy.
23. Temple University Libraries, "Confidentiality of Patron Records," last updated January 31, 2017, https://library.temple.edu/policies/confidentiality-of-patron-records.
24. Southern Illinois University Morris Library, "Patron Privacy Policy."
25. San Diego State University Library, "Freedom of Access and Privacy," https://library.sdsu.edu/about-us/policies-guidelines/freedom-access-privacy.
26. University of Denver Libraries, "Your Privacy and University Libraries," https://library.du.edu/policies/records-privacy.html.
27. East Greenbush Community Library, "Privacy Policy," https://eglibrary.org/about/policies/#privacy.
28. Fairbanks North Star Borough Public Libraries, "Borrowing Services," Policies and Procedures, last updated November 21, 2018, https://fnsblibrary.org/about/polpro/.
29. Geauga County Public Library, "Retention of Circulation Records," Geauga County Public Library Operating Policy Manual, December 17, 2019, http://divi.geaugalibrary.net/wp-content/uploads/2020/01/712-Retention-of-Records.pdf.

30. Queens Borough Public Library, "Privacy Policy," December 2003, https://www.queenslibrary.org/about-us/library-policies/privacy.
31. Brown County Library, "Privacy and Confidentiality," May 15, 2014, https://www.browncountylibrary.org/wp-content/uploads/2012/09/H_1-Privacy-and-Confidentiality.pdf.
32. Jessamine County Public Library, "Information Security Policy," last updated August 21, 2019, https://jesspublib.org/wp-content/uploads/3.6-Information-Security-Policy-2019-09-25.pdf.
33. Las Vegas–Clark County Library District, "Patron Privacy Policy."
34. San José Public Library, "Privacy Policy," last updated March 12, 2018, https://www.sjpl.org/privacy-policy.
35. San Diego State University Library, "Freedom of Access and Privacy."
36. Berkshire Athenaeum, "Guidelines for Confidentiality While Cooperating with Law Enforcement," 2010, https://static1.squarespace.com/static/5c7eed16e8ba44443d295e02/t/5cb177cdeb39315a7ce00238/1555134414545/BA_LawEnforcement_Confidentiality.pdf.
37. Cornell University Library, "Library Practices."
38. Harvard Library, "Harvard Library's Privacy Statement," Privacy, Terms of Use and Copyright Information, https://library.harvard.edu/privacy-terms-use-copyright-information#privacy.
39. University of Texas Libraries, "Privacy and Confidentiality."
40. University at Albany Libraries, "Internet Privacy Policy," https://library.albany.edu/privacy.
41. Southern Illinois University Morris Library, "Patron Privacy Policy."
42. Rutgers University Libraries, "Privacy Policy," October 19, 2010, https://www.libraries.rutgers.edu/privacy_policy.
43. Warrenville Public Library District, "Confidentiality of Library Records," Policy No. 420, www.warrenville.com/about/Policies/420ConfidentialityofLibraryRecords.pdf.
44. Berkshire Athenaeum, "Guidelines for Confidentiality."
45. Ocean County Library, "Computer Use and Internet Policy," last updated June 17, 2014, http://theoceancountylibrary.org/sites/default/files/internet%20policy.pdf.
46. Durham County Library, "Privacy Policy," July 2019, https://durhamcountylibrary.org/about/policies/privacy-policy/.
47. Tampa-Hillsborough Public Library, "Access to Electronic Resources," Policy No. LS 306, June 2018, https://www.hcplc.org/thpl/policies/300/LS306-Access-to-Electronic-Resources.pdf.
48. San José Public Library, "Privacy Policy."
49. Texas State University Libraries, "Virtual Reference Policy (Ask a Librarian @Alkek)," https://www.library.txstate.edu/about/policies/virtual-reference.html.
50. Temple University Libraries, "Virtual Reference Privacy Guidelines," https://library.temple.edu/services/privacy.
51. Southern Illinois University Morris Library, "Patron Privacy Policy."
52. Brown County Library, "Privacy and Confidentiality."
53. Berkshire Athenaeum, "Guidelines for Confidentiality."
54. Western Plains Library System, "Video Surveillance Policy," July 13, 2018, http://wplibs.com/wp-content/uploads/2018/10/Video-Surveillance-Policy.pdf.
55. Deer Park Public Library, "Security Camera Policy," last updated October 24, 2018, https://deerparklibrary.org/wp-content/uploads/2018/10/Security-Camera-Policy-Revised-Oct-24-2018.pdf.
56. Mount Prospect Public Library, "Video Surveillance Policy," 2019, https://mppl.org/wp-content/uploads/2019/05/Video-Surveillance-Policy-052919.pdf.
57. Ocean County Library, "Camera Surveillance," Policies, Fees and Forms, last updated April 19, 2016, https://theoceancountylibrary.org/policies-fees-forms.
58. Las Vegas–Clark County Library District, "Patron Privacy Policy."
59. Jessamine County Public Library, "Information Security Policy."
60. Brown County Library, "Privacy and Confidentiality."
61. Pinellas Public Library Cooperative, "Public Services Policies," May 31, 2019, www.pplc.us/misc-pdf/CirculationPolicy_2019.pdf.
62. Durham County Library, "Privacy Policy."
63. Nashville Public Library, "Social Media and Blog Guidelines for Using, Commenting, and More," https://library.nashville.org/about/policies/social-media-and-blog-guidelines.
64. St. Louis Public Library, "Social Media Guidelines," last updated April 3, 2017, https://www.slpl.org/service-policies/social-media-policy/.
65. Hillsborough County Public Library Cooperative, "Social Media Guidelines," Policy Number LS 1108, August 2018, https://www.hcplc.org/thpl/policies/1100/LS1108-Social-Media-Guidelines.pdf.
66. University of Connecticut Library, "Policy on Confidentiality of Library Client Records," https://lib.uconn.edu/about/policies/policy-on-confidentiality-of-library-client-records/.
67. University of California San Diego Library, "Privacy Policy."
68. Syracuse University Libraries, "Privacy Policy," version 2.0, last updated October 4, 2013, https://library.syr.edu/policy/documents/privacy-policy.pdf.
69. Temple University Libraries, "Confidentiality of Patron Records."
70. Cherokee Regional Library System, "Records Retention Policy," July 30, 2015, https://www.chrl.org/wp-content/uploads/2015/04/Records-Retention-Policy_Approved-July-30-2015.pdf.
71. Genesee District Library, "GDL Policy 6.9: Records Retention," *Policy Manual* (Flint, MI: Genesee District Library, 2016), https://www.thegdl.org/wp-content/uploads/Policies/Policy-Manual-for-Website.pdf.
72. San José Public Library, "Privacy Policy."

Chapter 6

Higher Authorities and the Potential Release of Information

The preceding chapters have focused on how library privacy policies address types of data collected, how it is used, and data security and retention. This concluding chapter focuses on higher authorities that libraries should be responsive to and circumstances in which collected data may be released. Higher authorities can include

- professional organizations
- parent organization policies; system-wide or consortia policies
- state and federal law

To some degree, these authorities can influence library privacy policies and dictate circumstances under which private information might be released.

Professional Organization Guidance, Recommendations, and Advocacy

This issue of *Library Technology Reports* has provided references to some of the privacy-related advocacy work from the American Library Association and other organizations. In these brief final reflections in this chapter, professional organizations can be considered a higher authority in the sense that they provide recommendations and guidance reflecting long-standing professional values. Policies from at least twenty-four of the academic and fifteen of the public libraries analyzed made reference to ALA documents and work. For example, the Ann Arbor District Library's policies make reference to the following ALA documents:

- *Access to Digital Information, Services and Networks: An Interpretation of the Library Bill of Rights*[1]
- *Privacy: An Interpretation of the Library Bill of Rights*[2]
- *Importance of Education to Intellectual Freedom: An Interpretation of the Library Bill of Rights*[3]
- *Code of Ethics of the American Library Association*[4]
- American Library Association's "Library Bill of Rights in Cyberspace"[5]

At sixty-three words, Colby College Libraries had the shortest identified library-specific privacy policy of the fifty academic libraries analyzed, and its policy notes,

> The Colby College Libraries adhere to the American Library Association (ALA) standards and ethics of facilitating, not monitoring, access to information. We do not collect information about patron activities beyond what is basic and necessary to conduct and fulfill the mission of the library. For additional information, please consult the ALA Library Bill of Rights.[6]

Another example of a policy referencing ALA work is the University of Oregon Libraries' privacy policy, which at the end provides a link to ALA's Privacy Tool Kit and mentions the ALA Office of Intellectual Freedom:

> This Statement has been adapted from the ALA Library Privacy Policy model, http://www.ala.org/advocacy/privacyconfidentiality/toolkitsprivacy/libraryprivacy, and was reviewed March 2015 by the ALA Office of Intellectual Freedom in order to confirm adherence to foundational library privacy principles.[7]

Parent Organization Policy

Libraries are not islands unto themselves. Both academic and public libraries may be responsive to library consortia or to shared system-level policies. Public libraries are typically responsive to a board of trustees that approves policy and serves in the public interest. Academic libraries are often subject to parent university or college policies, and in some cases policies associated with a broader university system. This research intentionally did not encompass parent-level policies, but numerous—perhaps all—parent universities have privacy-related policies. Approximately thirty of the academic library policies analyzed referenced corresponding university- or system-level policies or guidelines. Parent institution policies that often contain privacy aspects include

- data and website privacy, protections, practices, and governance (including information access policies and access-to-student-information policies and guidelines, among them policies and practices responsive to federal law such as FERPA)
- expected behavior and conduct policies related to the use of technology and licensed resources
- professional standards and business conduct policies
- cybersecurity policies
- privacy and confidentiality policies associated with sponsored programs and research subjects
- protected health information policies (including policies and practices responsive to federal law such as HIPAA)
- e-mail and mass communications policies

Some academic library privacy policies specifically note how other entities at the same institution may have different privacy-related practices. For example, Indiana University Libraries' policy notes,

> This privacy notice applies only to the Indiana University (IU) Libraries and explains our practices concerning the collection, use, and disclosure of user information. . . .
>
> Other units at the University may collect and use visitor information in different ways. Therefore, visitors to other University web sites and those who interact with University units and departments should review the privacy notices for those units or for the particular University web sites they visit. The IU Libraries are not responsible for the content of other web sites or for the privacy practices of University units or web sites outside the scope of this notice.[8]

Several academic library privacy policies note that the library's IT infrastructure or computer labs are managed by its university's centralized IT organization or mention other custodians of private information, such as a campus safety department. Oftentimes, the library policy refers users to this other campus entity for associated policies, questions, or concerns. For example, the University of Denver Libraries' policy notes,

> Security cameras and security doors . . . are located throughout the Libraries and are managed by Campus Safety; the Libraries are not privy to the data collected by these systems. Information Technology provides wireless internet routers through the building, as well as zero-client workstations. Cell phones often automatically "ping" wireless routers and exchange data (this is true wherever you go), and when you log into campus networks your campus ID is needed to authenticate. Please see IT@DU's policies and feel free to contact them if you have questions.
>
> Although these data are not collected or maintained by the Libraries, it is important to know all these systems are also subject to DU's Privacy Statement.[9]

Some library privacy policies reference higher level, system-wide policies. For example, the University of California Berkeley Library makes reference to the University of California system's *Electronic Communications Policy* and "RMP-8: Requirements on Privacy of and Access to Information."[10] While not necessarily higher level entities, other groups, such as a university's student government organization, can influence policy development. For example, the University of Texas Libraries' policy notes, "Developed in consultation with Student Government."[11]

Policies of library consortia represent another instance of what could be considered a higher level policy. Several public library policies note consortia policies or practices. For example, the Pinellas Public Library Cooperative in Florida consists of fourteen member libraries and has a public services and circulation policy that notes,

> Although each member library is operated by a separate local governmental unit or board which retains authority over any policy decisions for internal operations and the handling of local funds, member libraries have agreed, wherever possible, to work together to establish consistent public service policies. In keeping with the intent of the Interlocal Agreement, which supports member libraries' autonomy, individual libraries may establish additional service policies. Therefore,

> variations in official policies and procedures may exist between libraries.[12]

State and Federal Law

A very common component of many library privacy policies is references to legal statutes, often to statute-level privacy protections for library records and circumstances under which private information can be released. Legal statutes exist at the local, state, and federal levels. Regarding state-level statutes, as noted in ALA's "State Privacy Laws Regarding Library Records," "Forty-eight states and the District of Columbia have laws protecting the confidentiality of library records. Two states, Kentucky and Hawaii, have attorney general's opinions protecting library users' privacy. The language of these provisions var[ies] from state to state."[13]

Present federal-level statutes are rather lacking or outdated, increasing the complexity of privacy considerations. To note but one example—social media services—Lamdan noted,

> A lack of cohesive statutes on Internet privacy leaves a mere patchwork of inconsistent laws for social media outlets to follow. . . . Scattered and inconsistent state laws deal with tiny facets of social media privacy in different ways, but there is no comprehensive 50-state solution to social media's privacy invasions in the legal framework of the United States.[14]

Discussing recent initiatives at the federal level, Orlofsky noted,

> Members of the Congressional House and Senate subcommittees have been working for the past few years on different bills related to privacy. Given the impetus of the California law, the European Union's General Data Protection Regulation, and newsmaking data breaches such as the 2018 Facebook/Cambridge Analytica scandal, there has been recently a greater push to construct a national data privacy law. . . . One stated reason for a federal law would be to prevent a patchwork of state laws that offer varying levels of protection.[15]

Orlovsky's blog post provides additional information on existing and proposed federal statutes related to consumer protections. Such work is high on the radar of professional associations, such as the Association of College and Research Libraries (ACRL). Consumer data privacy ranks fourth out of five priorities on ACRL's legislative agenda focus for 2020.[16] In discussing this focus, ACRL notes that states continue to work on consumer data privacy laws. The agenda notes recently introduced Congressional bills under consideration. At time of writing, the potential of updated consumer privacy protections materializing at the federal level remains uncertain. As noted in the ACRL legislative agenda, "The ongoing concern over the erosion of individual privacy and predatorial online data mining practices warrants attention, engagement, and advocacy for government protections of the individual's right to privacy."[17] ALA's Privacy Tool Kit offers additional substantive content to inform the conversation. ALA's "Privacy and Confidentiality Q&A" notes, "Library policies must not violate applicable federal, state, and local laws. However, in accordance with Article IV of the 'Library Bill of Rights,' librarians should oppose the adoption of laws that abridge the privacy rights of any library user."[18]

ALA's extensive guidelines and checklists make various references to the law and the closely associated topic of enforcement-related requests for private patron information. Examples include the following:

"Library Privacy Checklist for Library Management Systems/Integrated Library Systems"

> Develop procedures for library staff on how to handle law enforcement and government requests for patron records.[19]

"Library Privacy Guidelines for Vendors"

> Libraries and vendors must work together to ensure that the contracts and licenses governing the collection, processing, disclosure, and retention of library user data reflect library ethics, policies, and legal obligations concerning user privacy and confidentiality.
>
> . . .
>
> In addition, agreements between libraries and vendors should reflect and incorporate restrictions on the potential dissemination and use of library users' records and data imposed by local, state, and federal law.[20]

"Library Privacy Guidelines for Library Management Systems"

> **Government Requests**
>
> The library should develop and implement procedures for dealing with government and law enforcement requests for library patrons' personally identifiable information and use data held within the LMS. The library should consider a government or law enforcement request only if it is issued by a court of competent jurisdiction that shows good

cause and is in proper form. The library should also inform users through its privacy policies about the legal conditions under which it might be required to release personally identifiable information.

The library could consider publishing a warrant canary notice to inform users that they have not been served with a secret government subpoena or national security letter. If a canary notice is not updated or it is removed, users can assume that a subpoena or national security letter has been served.[21]

"Developing or Revising a Library Privacy Policy"

In addition, policy drafts should be reviewed against existing local policies, state and local laws, and ALA recommendations and guidelines.

. . .

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 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.[22]

ALA's "Library Privacy Talking Points: Key Messages and Tough Questions" notes,

- 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.

. . .

- 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.[23]

In terms of the policies analyzed, references to municipal-level ordinances are rare, but one example is Lanesboro Public Library's "Data Privacy Policy," which notes,

> This policy will provide the guidelines and framework for library staff members to appropriately protect patron privacy and handle requests for public data. All City of Northfield policies and procedures related to government data also apply at the library. However, this additional policy is necessary to address data practices that are unique to the library.[24]

Conversely, at least forty-five academic and forty-four public libraries had policies referencing state or federal law. Georgia Tech Library's identified library privacy policy appears exclusively composed of references to Georgia law (the official Code of Georgia),[25] and there were several other instances where an academic library privacy policy was primarily composed of references citing state law. Several policies make reference to freedom of information statutes (which can vary across states). For example, the University of Michigan's "Library Privacy Statement—Frequently Asked Questions," notes,

Can data be obtained through a FOIA request?

The Michigan Freedom of Information Act is a broad disclosure law that requires the University to make many of its records publicly available upon request. Library records, however, get special protection under Michigan Law, which specifically shields library records from FOIA. A "Library record" is a document, record, or other method of storing information retained by a library that contains information that personally identifies a library patron, including the patron's name, address, or telephone number, or that identifies a person as having requested or obtained

> specific materials from a library. Deidentified and aggregated data that does not include identifying material is not protected by Michigan Law and is subject to FOIA.[26]

Several public library policies reference how circulation, registration, or other information tying an individual to materials is confidential and not considered a public record. For example:

Cherokee Regional Library System

> Circulation records and similar records of a library that identify the user of library materials shall not be public records but shall be confidential and may not be disclosed except under the conditions established under Georgia Law, Code 24-9-46.[27]

Ocean County Library

> Library records are still considered confidential under this law and require a subpoena issued by a court before release. Types of materials that would require immediate access are budgets, bills, vouchers, contracts, including collective negotiations agreements and individual employment contracts, and public employee salary and overtime information.[28]

Jessamine County Public Library

> **What constitutes a public record?** "Public record" means all books, papers, maps, photographs, cards, tapes, discs, diskettes, records, or other documentary materials prepared, owned, used, in the possession of, or retained by the Library. It does not include any records owned by a private person or corporation that are (a) in the possession of the Library or one of its employees and (b) do not relate to any function, activity, program, or operation funded by the state.[29]

Several public library policies reference how social media content is subject to public record law. For example, the St. Louis Public Library's policy notes,

> The content of the Library's social media is subject to public records laws, including the Missouri Sunshine laws. Relevant record retention schedules apply to social media content. Content must be managed, stored, and retrieved to comply with open records laws and e-discovery laws and policies.[30]

Some policies note that e-mail addresses are public records. For example, the Pinellas Public Library Cooperative's policy notes,

> Under Florida law, e-mail addresses are public records. If you do not want your e-mail address released in response to a public-records request, do not send electronic mail to this entity. Instead, contact this office by phone or in writing.[31]

Illustrating how state laws can vary (in this instance, between Florida and Oregon), the University of Oregon Libraries' policy notes that state law prevents e-mail addresses from public disclosure: "Oregon Revised Statute 192.502 (23) exempts from disclosure under open records law the records of a library, including . . . the electronic mail address of a patron."[32]

Of course, federal law represents the highest authority. As noted in Lanesboro Public Library's policy,

> Although state privacy laws regarding privacy in libraries are still in force, including laws protecting the confidentiality of library records, as federal laws the provisions of the Foreign Intelligence Surveillance Act (FISA), the Electronic Communications Privacy Act (ECPA), and the statute authorizing National Security Letters can supersede state privacy laws.[33]

The USA PATRIOT Act was referenced in at least fourteen academic and eleven public library policies analyzed. ALA's USA PATRIOT Act web page provides substantive information on the USA PATRIOT Act.[34] Several policies also reference the US Constitution. For example, Van Horne Public Library's policy notes,

> Confidentiality is essential to protect the exercise of First and Fourth Amendment rights. In accordance with First and Fourth Amendments of the U.S. Constitution, the Iowa Code and professional ethics, the Board of Trustees of the Van Horne Public Library respects the privacy of users and recognizes its responsibility to protect their privacy.[35]

Several policies provide detailed information on library procedures for how legal inquiries are handled. Perhaps the best example is the University of Utah J. Willard Marriot Library's privacy policy, which references

- procedures for how staff should respond to a law enforcement officer
- the role of university counsel
- the need to inventory any items viewed or confiscated as well as associated costs
- the requirement to call the ALA Office for Intellectual Freedom about the visit, if allowed
- the differences between search warrants issued by a FISA court and by a non-FISA court[36]

Several public library policies also provide details on their procedures, such as the Sequoyah Regional Library System, which has a policy noting that the library's executive director is the official custodian of records and outlines a detailed process flow and procedures should the library receive a request for confidential information.[37] The San José Public Library's policy appears to be the only one of those analyzed that includes a canary notice:

> This library has not been served with a government subpoena or national security letter under Section 215 of the USA PATRIOT ACT. If this notice is removed, customers can assume that a subpoena or national security letter has been served.[38]

Release of Information

Responding to an official law enforcement request is the most frequently mentioned circumstance under which private information might be released. Policies frequently note that the request must be a subpoena, search warrant, other court order, or otherwise required by law. A few policies note there may be exceptions in an emergency situation, when an official document in proper form is not practical. For example, Mount Prospect Public Library's "Circulation Policy and Library Records Confidentiality Policy," referencing Illinois public statutes, notes that certain information could be subject to release without a court order to a sworn law enforcement officer in an emergency or imminent danger situation and quotes the state law.[39] The policy includes an appendix reproducing the form the officer must sign to obtain the information. A large majority of library policies note that things must be in "proper form." As just one example, the San José Public Library's policy notes,

> Library records are not made available to any agency of state, federal, or local government without a subpoena, warrant, court order or other legal document requiring us to do so. These orders must show good cause and be in proper form.[40]

In addition to other references found within its policy, the Queens Borough Public Library's policy includes an overarching statement:

> Queens Public Library recognizes that law enforcement agencies and officers may occasionally believe that library records contain information which may be helpful to the investigation of criminal activity. If there is a reasonable basis to believe such records are necessary to the progress of an investigation or prosecution, the American judicial system provides the mechanism for seeking release of such confidential records. Library records will not be made available to any agency of state, federal, or local government except pursuant to such process, order, or subpoena as may be authorized under the authority of, and pursuant to, federal, state, or local law relating to civil, criminal, or administrative discovery procedures or legislative investigatory power.[41]

Policies may include other reasons why information might be released. Several reference the possibility of information release to prevent the threat of significant body harm or loss, to answer a threat to the personal safety of users, or to protect library property. For example,

> Josephine Louise Public Library—Walden, New York Web sites will disclose your personal information, without notice, only if required to do so by law or in the good faith belief that such action is necessary to: (a) conform to the edicts of the law or comply with legal process served on Josephine Louise Public Library—Walden, New York or the site; (b) protect and defend the rights or property of Josephine Louise Public Library—Walden, New York; and, (c) act under exigent circumstances to protect the personal safety of users of Josephine Louise Public Library—Walden, New York, or the public.[42]

At least nine academic library policies note the potential disclosure of information related to investigations of suspected misuse of systems or violations of university or library policies. At least fourteen academic and nine public library policies note that information can be released upon user consent (and many indicate the consent has to be in writing). Regarding children, at least eight academic library policies reference the rights of parents and legal guardians who request the release of a child's information. At least nineteen public library policies state whether parents do or don't have access to the records of their minor child, and further, many specify an upper age where this can happen. Some public library policies specify whether such access is full access to the record (such as specific titles checked out) or more generalized information (such as number of items checked out, but not the titles). Several also detail the circumstances under which this information can be released to the parent (e.g., some libraries will release the information only if the materials the child has checked out are overdue and accruing fines). Many public libraries specifically cite state law as regards the release of information related to minors. Examples include the following:

Pinellas Public Library Cooperative

> In accordance with FL Statute 257.261 (B.2), library staff hold all registration and circulation records confidential and will not surrender them or make them available to the public except by a properly executed court order, although circulation information may be disclosed to the parent or guardian of a cardholder under age 16 only for the purpose of collecting fines or recovering overdue library materials.[43]

Contra Costa County Library

> Library staff cannot give any information about a patron's registration and circulation record to anyone other than the patron, no matter what the age or relationship to the patron. For example, a parent cannot be told what material a child has checked out on the child's card without the child's consent.[44]

San José Public Library

> If the library cardholder is under the age of 18, the parent or guardian listed in the library record may only be given limited information about that child's record. Proof of the parent or guardian's identity is required through photo identification. Library staff will only tell customers the number of books checked out, due dates, and fines owed.[45]

Deer Park Public Library

> Children's records have the same confidentiality protection under New York Civil Practice Law and Rules, section 4509. Parents may pay fines and receive information as to the number of items a minor child, under 18, has checked out only with the child's card number, (telephone request), and with the child's card at the Library. Specific title and reserves are not accessible to the parent/guardian of a minor child. Parents/guardians who do not wish their children's records to remain private should check out materials on their own cards.[46]

In ending this chapter on higher authorities and circumstances under which private information may be released, the privacy policy of the University of New Mexico Libraries provides a fitting conclusion. Their concise privacy policy includes bulleted references to many categorical items discussed within this chapter—professional organization standards, parent institution policies, state law, and federal law. Their policy includes bulleted references to the following:

- professional standards from the American Library Association (with two documents noted)
- University of New Mexico policies (with two items noted, related to acceptable computer use)
- State of New Mexico law (with two statutes noted)
- United States law (with three federal statutes noted)[47]

Notes

1. American Library Association, *Access to Digital Resources and Services: An Interpretation of the Library Bill of Rights* [formerly titled *Access to Digital Information, Services, and Networks*] (Chicago: American Library Association, 1996, amended 2005, 2009), www.ala.org/advocacy/intfreedom/librarybill/interpretations/digital, cited in Ann Arbor District Library, "Internet Use Policy," Materials Selection and Access, last updated February 17, 2014, https://aadl.org/aboutus/materials.
2. American Library Association, *Privacy: An Interpretation of the Library Bill of Rights* (Chicago: American Library Association, 2002, amended 2014, 2019), www.ala.org/advocacy/sites/ala.org.advocacy/files/content/intfreedom/librarybill/interpretations/privacyinterpretation.pdf, cited in Ann Arbor District Library, "Internet Use Policy."
3. American Library Association, *Advocating for Intellectual Freedom: An Interpretation of the Library Bill of Rights* [formerly titled *Importance of Education to Intellectual Freedom: An Interpretation of the Library Bill of Rights*] (Chicago: American Library Association, 2009, amended 2014), www.ala.org/aboutala/sites/ala.org.aboutala/files/content/governance/policymanual/Links/B.2.1.21.pdf, cited in Ann Arbor District Library, "Internet Use Policy."
4. American Library Association, *Code of Ethics of the American Library Association* (Chicago: American Library Association, 1939, amended 1981, 1995, 2008), www.ala.org/advocacy/sites/ala.org.advocacy/files/content/proethics/codeofethics/Code%20of%20Ethics%20of%20the%20American%20Library%20Association.pdf, cited in Ann Arbor District Library, "Code of Ethics," Philosophical Statements, Ann Arbor District Library Policy Manual, https://aadl.org/aboutus/Philosophical#ETHICS.
5. American Library Association, "Library Bill of Rights in Cyberspace," cited in Ann Arbor District Library, "Ann Arbor District Library Internet Policy," last updated June 19, 2006, https://aadl.org/aboutus/policies/internet.
6. Colby College Libraries, "What Are the Privacy Policies in the Library?" Guidelines and Policies, https://www.colby.edu/libraries/about/guidelines-and-policies/.
7. University of Oregon Libraries, "UO Libraries Privacy Statement," last updated March 3, 2020, https://library.uoregon.edu/policies/privacystatement.
8. Indiana University Libraries, "Indiana University Libraries Privacy Policy," last updated February 1, 2012, https://policies.iu.edu/policies/lib-01-libraries-privacy/index.html.
9. University of Denver Libraries, "Your Privacy and University Libraries," https://library.du.edu/policies/records-privacy.html.

10. University of California, *Electronic Communications Policy* (Oakland: University of California, 2000, revised 2005), https://policy.ucop.edu/doc/7000470/ElectronicCommunications, University of California, "RMP-8: Requirements on Privacy of and Access to Information," policy rescinded November 13, 2015, https://policy.ucop.edu/doc/7020463/BFB-RMP-8, cited in University of California Berkeley Library, "Collection, Use, and Disclosure of Electronic Information," last updated September 22, 2008, https://www.lib.berkeley.edu/about/privacy-electronic-information.
11. University of Texas Libraries, "Privacy and Confidentiality of Library Records Policy," https://www.lib.utexas.edu/about/policies/privacy-and-confidentiality-library-records-policy.
12. Pinellas Public Library Cooperative, "Public Services Policies," May 31, 2019, www.pplc.us/misc-pdf/CirculationPolicy_2019.pdf.
13. American Library Association, "State Privacy Laws Regarding Library Records," www.ala.org/advocacy/privacy/statelaws.
14. Sarah Lamdan, "Social Media Privacy: A Rallying Cry to Librarians," *Library Quarterly: Information, Community, Policy* 85, no. 3 (2015): 266–67.
15. Vicky Ludas Orlofsky, "Consumer Data Privacy and the Federal Government," *Intellectual Freedom Blog*, March 27, 2019, https://www.oif.ala.org/oif/?p=17391.
16. Association of College and Research Libraries, "ACRL Legislative Agenda 2020," www.ala.org/acrl/sites/ala.org.acrl/files/content/issues/washingtonwatch/legislativeagenda20.pdf.
17. Association of College and Research Libraries, "ACRL Legislative Agenda 2020."
18. American Library Association, "Privacy and Confidentiality Q&A," last updated July 29, 2019, www.ala.org/advocacy/intfreedom/privacyconfidentialityqa.
19. American Library Association, "Library Privacy Checklist for Library Management Systems/Integrated Library Systems," last updated January 26, 2020, www.ala.org/advocacy/privacy/checklists/library-management-systems.
20. American Library Association, "Library Privacy Guidelines for Vendors," last updated January 26, 2020, www.ala.org/advocacy/privacy/guidelines/vendors.
21. American Library Association, "Library Privacy Guidelines for Library Management Systems," last updated January 26, 2020, www.ala.org/advocacy/privacy/guidelines/library-management-systems.
22. American Library Association, "Developing or Revising a Library Privacy Policy," Privacy Tool Kit, last updated April 2017, www.ala.org/advocacy/privacy/toolkit/policy.
23. American Library Association, "Library Privacy Talking Points: Key Messages and Tough Questions," January 2014, www.ala.org/advocacy/privacy/toolkit/talkingpoints.
24. Lanesboro Public Library, "Data Privacy Policy," February 2012, https://www.lanesboro.lib.mn.us/wp-content/uploads/2014/03/data-privacy.htm.
25. Georgia Tech Library, "Privacy Policy," https://www.library.gatech.edu/privacy-policy.
26. University of Michigan Library, "Library Privacy Statement—Frequently Asked Questions (FAQ)," last updated June 14, 2018, https://www.lib.umich.edu/library-privacy-statement/frequently-asked-questions.
27. Cherokee Regional Library System, "Privacy Policy," Policies and Laws, October 21, 2004, https://www.chrl.org/wp-content/uploads/2015/04/Privacy-Policy.pdf.
28. Ocean County Library, "Fines and Fees Schedule," Policies, Fees, and Forms, last revised April 19, 2016, https://theoceancountylibrary.org/policies-fees-forms#all_des544.
29. Jessamine County Public Library, "Open Records Policy," last updated June 24, 2019, https://jesspublib.org/wp-content/uploads/6.6-Open-Records-Policy-2019-06-24.pdf.
30. St. Louis Public Library, "Social Media Guidelines," last updated April 3, 2017, https://www.slpl.org/service-policies/social-media-policy/.
31. Pinellas Public Library Cooperative, "PPLC Privacy Policy," May 28, 2008, http://www.pplc.us/misc-pdf/PPLC_PrivacyPolicy.pdf.
32. University of Oregon Libraries, "Privacy Statement."
33. Lanesboro Public Library, "Data Privacy Policy."
34. American Library Association, "USA PATRIOT Act," www.ala.org/advocacy/advleg/federallegislation/theusapatriotact.
35. Van Horne Public Library, "Van Horne Public Library Policies," last updated January 8, 2018, https://www.vanhorne.lib.ia.us/library-information/policies/van-horne-public-library-policies-updated-1-8-18.doc/at_download/file.
36. University of Utah, J. Willard Marriott Library, "Privacy Policy," https://lib.utah.edu/pdf/Privacy_Policy_Procedures.pdf.
37. Sequoyah Regional Library System, "USA Patriot Act & Confidentiality of Library Records," MAN-1, Management Policies, Public Service Policy, last updated October 24, 2017, https://www.sequoyahregionallibrary.org/wp-content/uploads/2017/11/Public-Service-Policy-10.24.17.pdf.
38. San José Public Library, "Privacy Policy," last updated March 12, 2018, https://www.sjpl.org/privacy-policy.
39. Mount Prospect Public Library, "Circulation Policy and Library Records Confidentiality Policy," https://mppl.org/wp-content/uploads/2019/10/Circulation-Policy_all-docs-07-01-19.pdf.
40. San José Public Library, "Privacy Policy."
41. Queens Borough Public Library, "Privacy Policy," December 2003, https://www.queenslibrary.org/about-us/library-policies/privacy.
42. Josephine-Louise Public Library, "Privacy Statement," https://www.waldenlibrary.org/privacy.aspx.
43. Pinellas Public Library Cooperative, "1. Library Accounts—Registration Policies," in "Public Services Policies," May 31, 2019, www.pplc.us/misc-pdf/CirculationPolicy_2019.pdf.
44. Contra Costa County Library, "About Privacy," https://ccclib.org/policies/privacy/.
45. San José Public Library, "Privacy Policy."
46. Deer Park Public Library, "Library Patron Records Confidentiality Policy," February 23, 2011, https://deerparklibrary.org/wp-content/uploads/2017/06/Library-Patron-Records-Confidentiality.pdf.
47. University of New Mexico Libraries, "User Privacy Policy," July 6, 2016, https://elibrary.unm.edu/services/docs/library-privacy-and-confidentiality-policy.pdf.

Notes

Notes

Library Technology
REPORTS

Upcoming Issues	
October 56:7	**One Country One Library** by Mirela Roncevic
November/ December 56:8	**Consolidation in the Library Technology Industry and What It Means for Libraries** by Marshall Breeding
January 57:1	**Visualizing Digital Collections Data with R** by Monika Glowacka-Musial

Subscribe
alatechsource.org/subscribe

Purchase single copies in the ALA Store
alastore.ala.org

alatechsource.org

ALA TechSource, a unit of the publishing department of the American Library Association