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.