Pacific Library Partnership

LDH Consulting Services

DATA PRIVACY BEST PRACTICES TOOLKIT FOR LIBRARIES

A GUIDE FOR MANAGING AND PROTECTING PATRON DATA

SEPTEMBER 2020

plpinfo.org/dataprivacytoolkit

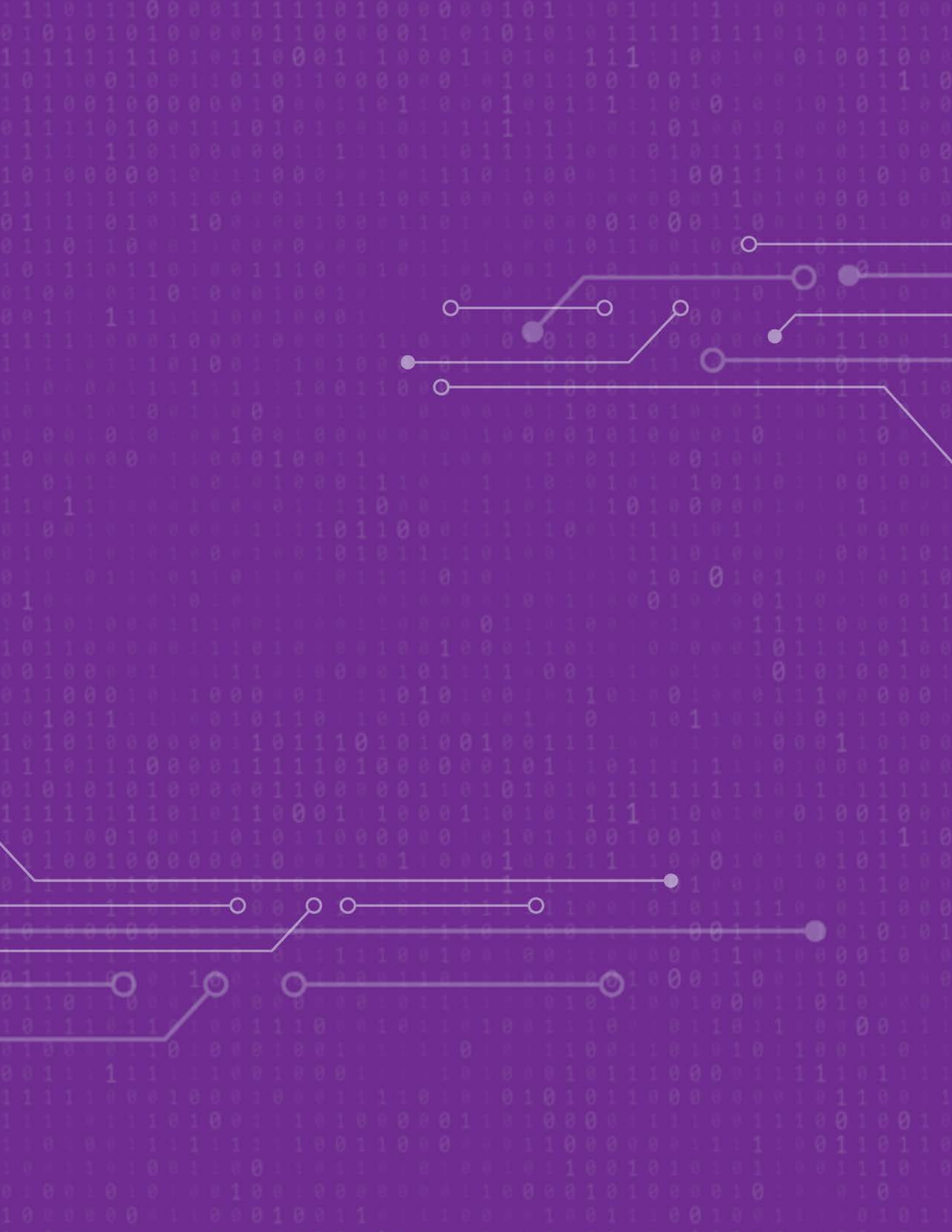


Table of Contents

Introduction and Project Background

The Data Privacy Best Practices Training for Libraries project was conceptualized by member libraries of the Pacific Library Partnership in FY 2019/20 as an LSTA grant funded project to develop and deliver three in-person privacy trainings and a privacy toolkit for PLP members, and to make these training materials available to other interested libraries that wish to modify the materials for their training purposes. With more services available online, patron privacy is critical and ever-changing for libraries. In addition, the California Consumer Protection Act of 2019 requires all vendors working with libraries to ensure patron data is secured and that it can be removed by the patron or by the library, under certain conditions.

The COVID-19 pandemic majorly impacted the project and required several major adjustments to the original goals for the project, including shifting of one of the three in-person trainings into a virtual format.

An initial needs survey and two focus groups defined the content for the two in-person training sessions in January and February of 2020 and the online training in May. Surveys from participants informed the data of this toolkit. There were a number of resources and issues that spanned a very wide range of privacy and security topics.

The toolkit's intended audience is wide-ranging, including administrators who want policy and contract guidance to front line workers who want practical advice about how to protect patron privacy in their daily work. The toolkit incorporates both high level and detailed information about building and maintaining all aspects of patron privacy program at the library. Three of the sections in the toolkit directly tie back to the three main training areas: the data lifecycle, operationalizing privacy at the library, and managing privacy with vendors. The remaining sections address topics not otherwise covered in the trainings, including specific patron privacy issues and considerations, public computing, and teaching privacy to patrons. At the end of the toolkit is an extensive resource section containing library privacy scholarship, professional standards, regulations, and a number of templates and examples libraries can use to develop their own contract addendums, privacy policies, and privacy workshops.

SECTION 1

WHY PRIVACY?

Privacy is Important in the Library Because…

Without privacy, there is no Intellectual Freedom. Without privacy, users wanting to seek out certain types of information without restrictions or consequences have to go elsewhere. There are not many other institutions beyond the library that uphold a person's right to privately access information without consequence.

Patrons have the right to privacy in the library. The American Library Association's Library Bill of Rights, Article VII, states:

All people, regardless of origin, age, background, or views, possess a right to privacy and confidentiality in their library use. Libraries should advocate for, educate about, and protect people's privacy, safeguarding all library use data, including personally identifiable information.

Legal regulations also grant patrons certain privacy rights. On a federal level, the 4th Amendment grants privacy protections from search and seizures. The US Supreme Court ruled in Katz vs United States in 1967 that the 4th Amendment protects people when there is a reasonable expectation of privacy. In California, Government Code Section 6267 protects both the data about a patron and about a patron's use of library resources from public disclosure. This protection not only covers data collected and stored by libraries, but agencies acting on behalf of a library, such as library vendors who work with patron data.

Patron privacy is an equity issue. Libraries serve a wide range of patrons from a variety of backgrounds: race, gender, ethnicity, class, religious beliefs, sexuality, immigration status, housing status, ability, incarceration status, and age. Patrons span from the most privileged in this society to the most vulnerable. Libraries provide people with opportunities to learn and grow in an environment that is safer for them to explore and experiment without major repercussions or judgement. For populations targeted by heightened surveillance and face the consequence of such increased surveillance, the library might be one of the only safer places for them to go to for this type of opportunity.

Telling Others Why Library Privacy is Important

A library works with and serves different people who have their own beliefs, values, and needs. Tailoring your communications to address your audience's needs and values will help create a connection between you and your audience in your privacy discussions.

A number of factors influence the effectiveness of any communication plan:

- *Your relationship to the target audience* — established relationships help provide a level of trust and understanding between all parties needed to have honest and productive privacy conversations.
- *Wording and language choices* — use of jargon, certain writing styles (such as legal text), and other composition choices (such as only offering an English language version of the text) can be barriers in communicating with your audience.
- *Needs and values* — target audiences have their own needs and values that might widely differ from your own, and sometimes conflicting within the audience itself.
- *Positive-sum verses "all or nothing" outcomes* — taking a "we can have privacy or we can have this other thing" approach to privacy discussions leaves little to no room for discussions that address the privacy needs and concerns of everyone involved.

Library privacy involves and affects a wide range of people. **Building a base of support for library privacy should include the following audiences:**

Within the library

- Library workers, from frontline workers at the circulation desk to library administration
- Library Board and Friends of the Library members

Within the larger organization

- External information technology departments
- City officials, such as the Mayor's office, Office of Civil Rights, Education, Human Services, Neighborhoods, etc.
- Academic administrators, such as Deans, Provosts, Presidents
- Staff, faculty, and student organizations and unions

With the public

- Library patrons
- Non-library users in the community
- Community organizations
- Advocacy groups

Each group has their own views on privacy in the library, as well as their own privacy needs and concerns. These needs and concerns can range from compliance to regulations and standards to concerns about personal safety. Building these relationships throughout time leads to not only a better understanding of each side, but also increases the effectiveness of the library's privacy measures in meeting the needs of their patrons and greater community.

SECTION 2

PATRON DATA LIFECYCLE

Please visit https://plpinfo.org/dataprivacy for training materials, resources, and template files referenced in this section, including those developed by PLP for this project.

Libraries and Patron Data

Library collect, store, retain, and process more patron data than they realize. Below is just a short list of where patron data lives in the library:

- Integrated library systems
- Database backups
- Print management systems
- Server logs
- Reference chat logs
- Public computer/wireless traffic logs
- Security camera footage
- Program attendance logs and surveys
- Paper forms
- Staff email
- Vendor applications and servers

The patron data collected by libraries is divided into two categories:

1. Data about a patron

- Name
- Address
- Email
- Date of birth
- Library barcode

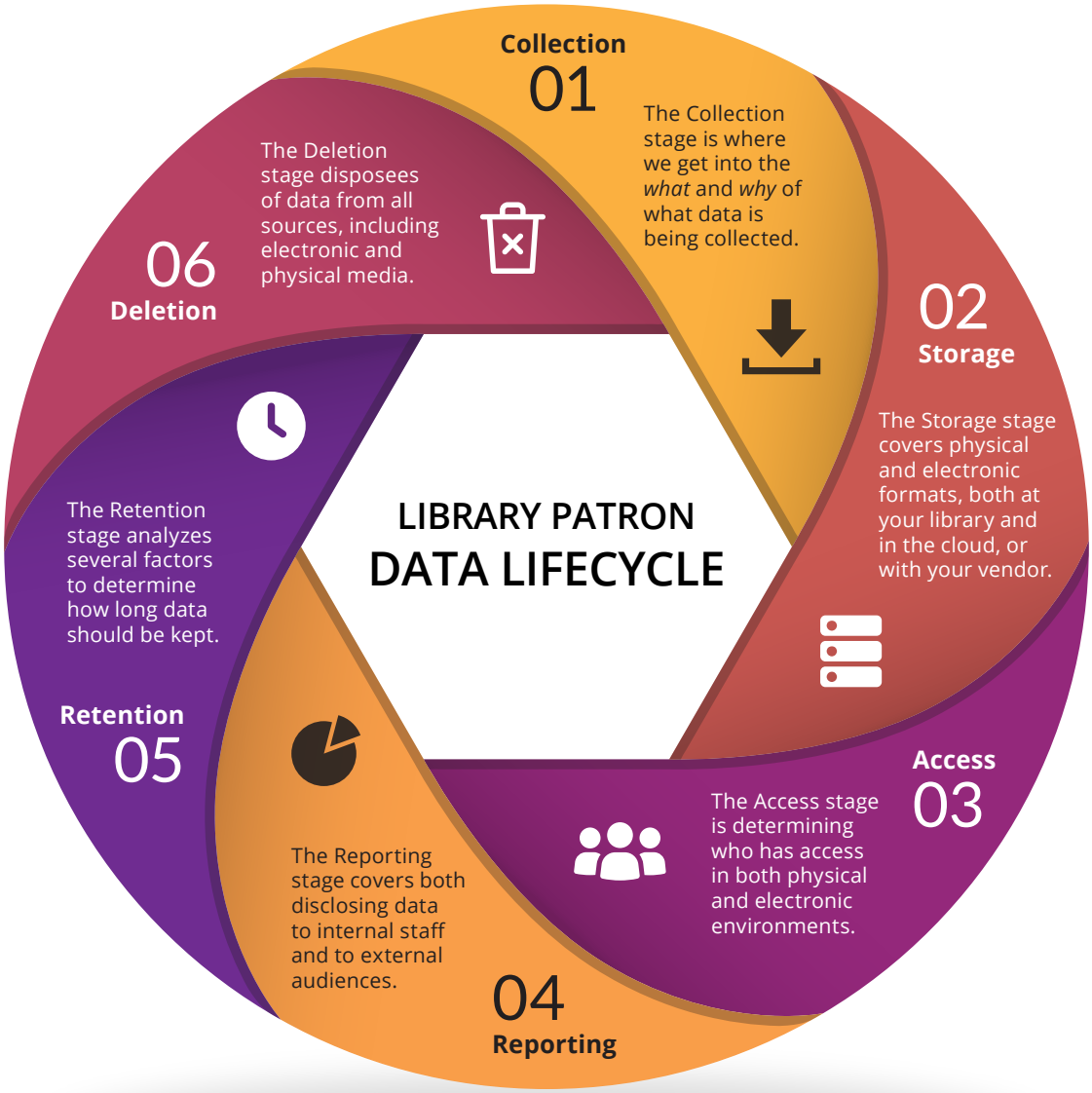
2. Data about a patron's activities in the library

- Circulation and search histories
- Public computer and Wi-Fi sessions
- Reference interactions
- Program attendance and feedback/surveys
- Access to electronic resources, including IP address and authentication logs

Without data, it is hard for a library to build and sustain support from administration, government officials, taxpayers, donors, and other groups that have a direct impact on the operations of the library. Nonetheless, how libraries go about data operations in their organizations determines the amount of possible harm experienced by both the patron and the library.

Library Patron Data Lifecycle

The patron data in the library goes through a lifecycle. There are six stages in the cycle: collection, storage, access, reporting, retention, and deletion. We can use the data lifecycle to identify key risks presented with your library's handling of patron data, as well as identify strategies in mitigating those risks.



Collection

WHAT DATA IS COLLECTED AND WHY

*The collection stage is one of the most important stages in the lifecycle. This is where we get into the **what** and **why** of what data is being collected.* ***If you don't have the data, it can't be leaked, breached, or otherwise improperly used by others.***

Privacy risks

- Not knowing what data is collected
  - Many library applications and systems collect more data than you realize. Servers and applications keep system logs of activity and by default collect PII information, such as IP address, a unique device id, timestamps, and transaction information, including search activity.
- Data FOMO [Fear of Missing Out]
  - We tend to collect data because we think it might be useful, though we do not have a demonstrated case as to why we are collecting it now.

Risk mitigation strategies

- Conduct data inventories (more information provided later in this section)
- Adopt data minimization — limiting your collection of personal data to only what is required to meet a specific business need. **If you do not have a *demonstrated* business case as to why you are collecting a data point, *then you should not collect that data point.***

The Five Whys

This method is useful to eliminate scope creep when determining what data to collect. When a person answers your first "why?," you then ask "why?" again, making the person think about the answer they gave the first time around, then they give you another answer building off of that one, and then you repeat the process until you get to the fifth "Why?" or your person can't answer "why" anymore — whichever comes first. This method has been used in other fields to get to root causes when evaluating problems, but this method is also useful to eliminate scope creep when determining what to collect.

Remember that sometimes a data collection issue is resolved by addressing the policy and procedure that is causing the issue.

02

Storage

WHAT DATA IS STORED AND WHERE

Storing data might seem simple, but data wants to be free. Storage covers physical and electronic formats, both at your library and in the cloud, or with your vendor.

Privacy risks

Data can be stored in a variety of places outside of their native applications and processes, including:

- Local computer hard drives
- Local network storage
- Third party cloud storage applications, such as Google Drive, Evernote, or Office 365
- Email
- Printouts on desktops, cabinets, drawers, and other physical storage or areas

You create an even higher risk if you store different raw data sets into one central place, building a profile of the patron's use of the entire library. If not done very carefully, this practice puts the entire notion of library patron privacy at risk.

Risk mitigation strategies

- Limit the number of places for storing raw patron data to the native processes and systems in which the data is collected.
- Restrict use of third-party cloud collaborative or storage solutions for collecting and storing raw patron data.

Storage option — data warehouses and data de-identification

A privacy-conscious approach to data warehousing includes not storing raw patron data in the warehouse, but instead de-identifying the data during the extract-transform-load process (ETL). Data de-identification methods include obfuscation, truncation, and aggregation.

De-identification is not fool-proof and must be approached with care. Many de-identification methods have varying re-identification risks. Many libraries have demographic outliers in their service populations or have small overall service populations, all of which makes many de-identification methods not viable for a good number of libraries. In addition, re-identification is possible if the data had enough lingering patron data — particularly data about a patron's activities — and is combined with other data sets.

Access

WHO HAS ACCESS TO DATA

The Access section helps you assess the various risks you should consider when granting physical or electronic access to patron data to others.

Physical access

- Desktop computers and laptops
- Mobile devices
- Server room/data center
- Offices, desks, and file cabinets
- Flash drives
- Security camera terminal and tapes

Electronic access

- User permissions
- Administrator account information
- Vendor access to local systems
- System log and database access
- Administrator site access

Privacy risks

Physical access risks mostly come in the form of not securing physical equipment or spaces that store patron data. Electronic access risks come in different forms:

- User permissions and roles — Major applications have varying levels of user permissions, or none
- Staff and vendor access changes — varying levels of access to systems and applications are needed, and often these changes do not happen or are missed

Risk mitigation strategies

The best ways to mitigate privacy risks in this stage is to follow best practices in information security:

- The Principle of Least Privilege — Users and programs can only access the data necessary for performing intended function or duty
- Restrict physical access through controlled-entry, including locked offices, cabinets, and desks
- Restrict electronic access:
  - Require logins to access staff applications and physical devices
  - Enable multi-factor authentication (MFA)
  - Require staff to log out or lock their computers when they are away from the computer
  - Encrypt hard drives and mobile devices
  - Add a remote wipe for mobile devices in case they are reported lost or stolen
- Conduct annual audits of:
  - user account access and roles in staff applications
  - who has physical and electronic keys to controlled entry spaces that contain patron data

See the resources section of the plpinfo.org/dataprivacytoolkit for additional security checklists and standards to better protect access to patron data.

Reporting

WHAT DATA IS DISCLOSED WITH WHO, AND WHY?

Reporting covers both disclosing data to internal staff and to external audiences, such as the public, third party vendors, and city or parent organization administration or staff.

Privacy risks

Two major areas of risk in reporting on patron data surround the *generation and disclosure* of the reports:

- Staff requesting (or having) unrestricted access to patron data to create reports
- Releasing improperly de-identified patron data in reports or in data sets (refer to the section about de-identification for risks of sharing data with others)
- Staff or third parties disclosing patron information without the patron's permission
- Staff being a "good citizen" or providing "good customer service," including
  - giving more information than requested under a warrant or subpoena
  - giving information to law enforcement without a court-issued order
  - giving patron data to other patrons on request outside of what is allowed by policy and procedure

Risk mitigation strategies

Your choices in the collection and storage of data impact what you can report out.

- Provide a data dashboard or "canned" reports that use aggregated patron data for the most requested or used reports for library reporting
- Restrict access to raw patron data by creating database views that contain transformed patron data for use by library staff for reporting
- Transform report data through additional obfuscation and aggregation methods
- Review data reporting and disclosure processes using a privacy impact assessment (see below for more information)
- Only disclose patron data under certain circumstances, including consent of the patron and by court-issued warrant
  - Only give data explicitly requested in the subpoena or warrant, and not volunteering additional information beyond that
- Consider not releasing patron data when it is impossible to protect the privacy of the individuals in the data set

Retention

HOW LONG DATA IS KEPT

How long you should keep data depends on several factors, including legal regulations and operational considerations.

Privacy risks

- **No policy —** There might not be a retention policy or schedule at your library, making it difficult to decide what should be kept and what should be deleted at what time
- **Non-compliance —** You might have policies and schedules in place, but your library might not in compliance with library policy or local or state regulations surrounding data retention schedules

Risk mitigation strategies

The best way to mitigate privacy risks in this stage is to create a retention schedule for library data that adheres to local and state policy and regulations, and consistently follow the schedule, as well as make you aware of any specific retention schedules applicable to your own organization or parent organization. Legal staff and records management staff for your library or parent organization can help you determine if there are any library data exceptions in public disclosure and record retention policies and regulations.

For data that is not subject to external retention schedule periods, the best practice in the length of retention is that **data should retained only for the length of time that the data is absolutely needed for operational or legal purposes.** A privacy impact assessment of a process or system that collects and stores patron data can assist in creating retention schedules by measuring the amount of risk each type of data carries if kept for a certain length of time due to operational needs.

06

Deletion

HOW DATA IS DELETED

Deletion of data includes disposal of electronic and physical media. ***Note that once you collect data, it becomes nearly impossible to delete all versions and copies of that data.***

Privacy risks

- You can't delete data just once. You have various versions of the data living in backups, printouts, spreadsheets, staff email, cloud services, and so on.
- Patron data can be retrieved on improperly discarded drives or with off the shelf programs available to the public
- Vendors might not delete patron data when no longer needed, or not follow standards on secure destruction of materials
- Paper documents that contain patron data can be retrieved via dumpster diving if not shredded or properly disposed

Risk mitigation strategies

- Properly dispose of physical media that contain patron data following secure media destruction standards, such as NIST SP 800-88, or contract with companies that specialize in secure media destruction to help with this process.
- Libraries should keep track of where patron data is stored through a regularly scheduled data inventory, and restrict storage of data exported from the original source
- Libraries should work with vendors in proper deletion of patron data in vendor systems, including conducting an annual privacy and security audit to determine any data missed during the deletion process

Identifying Patron Data Privacy Risks

When data is breached or leaked, both the library and the patron experience harm. The library can experience harm in the form of damage to the library's reputation, as well as legal penalties if the library failed to comply with regulations including regulations requiring notification to patrons surrounding the breach. Harm to the patron comes in many forms:

- The public release of patron data can lead to identity theft
- Users accessing information on certain topics, such as physical and mental health, religion, politics, and sexuality, can suffer real world consequences if others in their family or community find out about their library activities
- Law enforcement may gain access to collected data, which can have real-world consequences if the library is asked for data related to immigration, religious, or political status

There are two ways that libraries can identify and mitigate library data privacy risks: *data inventories* and *privacy impact assessments.*

Data inventory

Data inventories record what data is collected, where it is stored, how data is used and shared with others, as well as data ownership and governance. Libraries can use data inventories to map the data lifecycle in one system (like an ILS or web analytics application) or process (such as registering for a library card), or do a data inventory of the entire organization. A customizable data inventory template is available at the project website.

DATA INVENTORY CONSIDERATIONS:

- **Follow the data —** ask questions that can be directly tied back to one or more data lifecycle stage(s)
- **Ask around —** go beyond the person responsible for the system or process and include people who use the system/process as well as the data processed from the system/process
- **Build in accountability —** In addition to having an annual general data inventory of your organization, data inventories should be done whenever you bring a new product or process into the library, or when a process or product has a major change in any of the stages of the data lifecycle. Vendors should be instructed to do data inventories as part of their annual security and privacy audit or when major changes are made to their systems or processes.

Privacy impact assessment

A privacy impact assessment (PIA) provides a standardized way to comprehensively identify and assess different types of risk to patron privacy in data processing practices.

The three goals of a PIA:

- Evaluates new and existing processes for compliance to legal regulations and policies
- Assesses privacy risks presented by processes
- Identifies and examines possible ways to mitigate risks in processes

Like data inventories, PIAs are done anytime you bring a new system or process into the organization, as well as when there are any major changes to those systems or processes. PIAs generally follow four phases:

1. **Preparation —** This phase determines if you need to do a PIA in the first place. If the process or system you're evaluating touches patron data, then a PIA is most likely needed.
2. **Data analysis —** The analysis is like an expanded data inventory, documenting not only the flow of data, but also the nature of disclosure of the data to third parties, legal regulations governing data processing, and information security at every stage of the data lifecycle.
3. **Privacy Assessment —** After the analysis, it's time to assess the privacy risks associated with the process or system. **Risk** is the **potential cost** resulting from a **threat** taking advantage of a **vulnerability.** This stage also needs to take into consideration the level of impact if the risk is realized and the chances that the risk will happen.
4. **Reporting —** In risk management there are a number of ways you can respond to risk:
   - **Accept**
     The risk is considered low priority or unlikely to happen. *If you choose this response, document your rationale, as well as any potential consequences of when the risk is realized.*
   - **Transfer**
     The risk might be better managed outside of the current process or system and in places that are better equipped in handling the risk, such as an external department or tool
   - **Mitigate**
     Building in privacy controls in the process or system to lessen the chance of the risk being realized
   - **Eliminate**
     Changing the process or system to avoid the risk

Assigning a project team and coming up with a project plan to follow through on the report will ensure that your recommendations will be implemented. In addition, you will need to follow up afterwards on the changes you made to the product or service to determine if the risks were addressed with those changes.

SECTION 3

PATRONS AND PRIVACY

Please visit https://plpinfo.org/dataprivacy for training materials, resources, and template files referenced in this section.

Library workers routinely work with patrons in providing guidance about how to protect their privacy in and outside the library. The library's role in teaching privacy and security to patrons has grown in the past few decades with the rapid evolution of technology and the growing prevalence of the internet in daily life. This section covers ways that libraries can provide the tools and knowledge patrons need to protect their privacy, special considerations around certain patron privacy concerns, and strategies in talking privacy to patrons.

Teaching Patrons About Privacy

There is already good work by libraries in teaching privacy to patrons. Here are four types of programming or services your library should consider planning a patron privacy programs at your library.

Digital literacy

Many libraries offer some form of digital literacy programming, wither it be computer basics to navigating the internet. Other libraries focus on finding and evaluating information on the internet, including classes around disinformation and fake news. Digital privacy and security topics are a key component in these classes and can be tailored on the needs of the class.

Information security and privacy

Information security and privacy classes can be offered as a stand-alone program or as a compliment to other digital literacy classes in an overall program. While other classes can give patrons "just in time" information about privacy and security for a specific topic, dedicated classes allow patrons more time to explore and to have longer discussions around protecting their privacy. Because patrons have a wide range of technical skills and digital literacy awareness, the library should offer multiple classes based on skill and knowledge levels. Libraries should offer basic, intermediate, and advanced information security and privacy programming.

Device security

Library staff working public-facing desks have seen an increased number of patrons dropping in at the desk with questions about how to use a digital device, including smartphones, ereaders, and tablets. These one-on-one consultations at the information desk are an opportunity for library workers to provide "just in time" privacy and security instruction or information about the specific device to patrons.

Staff should have access to documentation regarding basic security and privacy features of models and versions of the most popular devices and applications. Staff can also create a small flyer for patrons to take with them that have basic security and privacy information and settings for popular devices, as well as information about where they can learn more about privacy and security for their device.

Privacy consultations

Several libraries, such as Cornell University Libraries, offer one-on-one privacy consultations for patrons who have specific questions regarding digital privacy or security. These scheduled appointments take advantage of the privacy and security skills of staff to offer a tailored service, though staff should not offer legal advice. These consultations can range from specific questions around specific device/application privacy and additional guidance on digital privacy to protecting sensitive research data or how to best protect the privacy of others while engaging in research or work.

Patron Privacy Concerns – Special Considerations

Each patron has their unique concerns about privacy in and outside of the library. A good illustration of these concerns and risks is documented in the ***Risk Assessment module of the Data Privacy Project*** *(https://dataprivacyproject.org/learning-modules/risk-assessment/)*. Library workers need to be aware that certain patron populations have privacy concerns that must be taken into consideration while planning privacy programming and operations at the library.

Meeting Mel and Rafaël

Mel and Rafaël are two of the many patrons that regularly visit the library. Most days you find Mel, a teen going to the local high school, sitting with their headphones on at one of the library computers while their little brother flips through the latest chapter book he found in the children's section. Mel and their little brother have been spending more time than usual at the library after their family moved into a shelter.

Rafaël finds social connections at the library. He regularly comes to the weekly Senior Coffee Social held in the meeting room to socialize with other seniors and to keep practicing his English after starting to learn the language a few years ago. Afterwards he reads the online local newspaper using the screen reader installed on the public library computers.

While many patrons have similar privacy needs and concerns, Mel and Rafaël have special privacy needs and concerns that the library also need to address to effectively protect their privacy.

Library Patron Mel

Mel's privacy considerations as a...

- **Student —** While the public library is not covered under the Family Educational Rights and Privacy Act (FERPA), any student data that the public library receives and processes from the school district must follow FERPA regulations. This includes not using the student data other than the purpose stated in the data sharing agreement and not disclosing student data to third parties, including other vendors. Academic and school libraries should consider library record information, including library use data attached to a student's name, as an educational record covered under FERPA (per recommendation by ALA).
- **Minor —** There are at least two areas of concern:
  - Libraries usually give parents and legal guardians access to their child's records. What information do the parents and legal guardians have access to? Depending on your library privacy policy, Mel might be entitled to the same privacy as adult patrons once they turned 13.
  - Any online vendor library services targeting Mel's younger brother need to follow the regulations around consent and data processing in the Children's Online Privacy Protection Act (COPPA). Online services must gain the parent's or guardian's permission before collecting the minor's data, and there are additional regulations around marketing and data processing.

- **Insecurely housed —** Now that Mel's family is temporarily living in a shelter, they might not have a permanent address for a while. What is the process of verifying addresses in the patron record? Mel might not have an ID card or one that has an address. Another consideration is if Mel's family moved to a shelter to escape a domestic abuse situation. In these situations, the library needs to work with the shelter to determine what address to use and how to handle situations where someone requests information from a patron record from someone staying at the shelter (particularly if the person is a parent or legal guardian of a minor staying at the shelter).

Library Patron Rafaël

Rafaël's privacy considerations as a...

- **Immigrant or undocumented person —** Because Rafaël migrated to the US, he might be a target for additional surveillance. *Under no circumstances should libraries collect or store data that can be tied back to a person's citizenship or immigration status.* Libraries must have policies and procedures in place for law enforcement requests, including requests from immigration agents who come into the library asking if a patron is in the building.
- **Patron with disabilities —** Patrons like Rafaël might ask for accommodations under the Americans with Disability Act (ADA) to use special equipment or for other accommodations. Libraries should not store medical information in the patron record or in other systems, such as staff email. Patron codes can be used to provide accommodations such as if a patron needs extended loan periods or changes to the limit of materials they can check out at once.

Talking With Patrons About Library Privacy

Clear, concise, and open communication with patrons about library privacy can help mitigate any misunderstandings or miscommunications of expectations between patron and the library. Here are some points to help with planning communications with patrons.

Considerations

- Publish privacy-related information in electronic and physical formats:
  - Electronic formats can include emails, social media posts, web site alerts and dedicated web pages
  - Physical formats include posters, flyers, handouts, and letters

- Conduct usability and accessibility testing on privacy website pages to ensure patrons can find the page and understand how the library is approaching privacy
- Publish content in the major languages of your patron community. Use human translators and not machine generated translations to avoid mistranslations and misunderstandings.
- Use plain language and limit use of acronyms and jargon to a minimum. Any unavoidable use of an acronym or jargon should be defined in the text.
- Take into account reading and language skills of your patrons. Library communications might not be accessible to some patrons who do not have strong reading or language skills.
- Talk with your community partners and work with them to facilitate discussion around library privacy concerns and programming for their members.
- Have a dedicated contact method, such as an email or contact person, so that patrons know where to go to if they have library privacy questions.

SECTION 4

OPERATIONALIZING PRIVACY AT THE LIBRARY

Please visit https://plpinfo.org/dataprivacy for training materials, resources, and template files referenced in this section.

Effective privacy operations require a comprehensive approach to privacy in library operations. Overall, effective privacy operations should:

Empower staff. Missing or insufficient policy and procedure, lack of training, and even little to no organizational support for professional development hamper staff ability to protect patron privacy.

Protect patrons from a variety of privacy risks. The library should consider how insufficient policy, procedure, and practice around what patron data the library collects, stores, and shares can harm patrons.

Mitigate your library's legal and financial liability when something goes wrong. You may have policies in place, but if there is no structure in place to consistently implement those policies then you could be found liable.

Embedded Privacy – Privacy by Design

Privacy by Design is widely used by organizations wanting a comprehensive approach to privacy in their everyday work. This is, in part, to avoid having privacy tacked on at the end of a process or project, where it's much harder to implement privacy effectively. Some Privacy by Design principles require organizations to approach privacy in an inclusive manner, while others require a shift in the framing of any privacy discussion. We tend to think that we can either have privacy or we have data needed to keep our libraries in business. By reframing privacy from a "this OR that" to a "this AND that," you can then focus privacy work on how to accommodate the needs and concerns of everyone involved without priming them for a figurative fight to get their needs met.

The next section breaks down how to approach privacy in all aspects of library operations.

Operationalizing Library Privacy

Before we begin...

POLICY, PROCEDURE, PRACTICE

Each library has a set of policies, procedures, and practices that they use for everyday operations at the library. Local practice is informed by procedure, procedure is informed by policy, and policy is informed by several factors such as legal regulations, industry standards, and best practices.

STAKEHOLDERS

Because library privacy operations affect everyone at the library, your privacy operations should address their needs and concerns. In any discussions that you have about policy, procedure, or practice, the following stakeholders should have some part in those discussions:

- Library administrators
- Legal counsel
- Library board
- Parent organization/institution
- Library staff
- Patrons
- Community partners
- Professional organizations
- State libraries
- Vendors

Policy

Policy is your "what" and "why" document. Policy provides the high-level framework for your organization's operations.

BEST PRACTICES

Privacy policies and **privacy notices** are important in setting the tone of your library's privacy program. Privacy policies refers to internal policies within your library. Privacy notices are for to your external audiences, such as library patrons and the public. Examples of notices and policies, as well as additional information about the minimum requirements for each type of policy and notice, can be found at https://plpinfo.org/dataprivacy.

A library must, at minimum, have a Library Privacy and Confidentiality of Library Patron Data Policy. This policy needs to address patron notice and consent, law enforcement request, and data processing at the library. Other library policies should have a privacy component that ties back to the main privacy policy, such as the use of third party vendor storage solutions, email use, and telecommuting.

A library must also, at minimum, have a publicly posted privacy notice that is accessible to all patrons. Privacy notices can share some of the same text as the privacy policy, but privacy notices need to be written for the public. Privacy notices should include information about what patron data is collected, processed, and disclosed; data protection and security measures taken by the library; and how patrons can access, modify, and delete their data at the library.

More libraries are creating a separate vendor privacy policy page for patrons. These pages list the privacy policies of the vendors the library does business with, including content providers and library applications such as the discovery layer, web chat applications, and the ILS.

CONSIDERATIONS

Legal regulations

Library patron data fall under a variety of different legal regulations. For California, Government Code Sections 6254 and 6267 protect patron data from public disclosure and require libraries and entities acting on behalf of a library to keep data about a patron as well as a patron's activities in the library confidential (respectively).

Two other California laws — the California Consumer Privacy Act of 2018 and Civil Codes around data breaches and incident responses — can also be addressed in tandem with the library's work with vendors who need to comply with those laws. School and academic libraries should address how they are meeting Family Educational Rights and Privacy Act (FERPA) compliance as library patron records can be considered educational records according to ALA. Libraries with minors under 13 years old will need to address how they are working with vendors who provide online services in protecting the minor's data under the Children's Online Privacy Protection Act, or COPPA.

Local regulations, particularly surrounding public disclosure and retention of data, should also be addressed in relevant privacy policies.

Policies – standards and best practices

Policies should incorporate professional standards and best practices surrounding patron data privacy and security. ALA provides US libraries with a number of professional standards, ethics, and guidelines, including their guidelines around surveillance technology guidance and law enforcement request guidance. IFLA, CLA, and the California State Library also have resources to help you frame your policies according to ethics and standards. The Fair Information Practice Principles (FIPPS) and the OECD Privacy Principles both have influenced ALA and other professional organizational recommendations and guidelines around privacy.

Your privacy policies should also draw from information security and privacy best practices, such as data minimization (limiting the collection of personal data to only what is required to meet a specific business need) and the Principle of Least Privilege (users and programs can only access the data necessary for performing intended function or duty).

Writing and publishing policy and notices

- Write for your audience. Having separate documents for staff and patrons will help best address each audiences' needs. Follow Section 3 about communicating to patrons when communicating to your patrons about privacy.
- Conduct usability and accessibility testing for online notices posted on the library website
- Conduct focus groups with staff and patrons during the drafting process

- Post the public privacy notice in conspicuous places in the library, as well as create pamphlets of the notice for patrons to take with them
- Privacy policies and resources should be in a centralized knowledge base where staff can access and contribute their experiences and knowledge surrounding the privacy policies.
- Communicate any changes to staff policies via email as well as regular team meetings, particularly those teams that are most impacted by the changes or have staff who do not have ready access to email or the staff intranet
- **Make sure that your privacy policy and privacy notice are aligned with each other.** Your privacy notice to your patrons must reflect the privacy policies you base your library's procedures and practices on.

Procedure

Procedure is the "how, when, where, and who" document. Procedure allows you to address specific concerns of implementing policy in departments or project groups.

BEST PRACTICES

Reviewing new or updated procedures against current privacy policies will ensure that the two types of documents are in alignment. This review should also happen when there are new or revised privacy policies.

Libraries should have at least the following procedures that tie back to privacy policies:

- Law enforcement requests for patron information, including asking if patrons are in the building
- Patron data requests from other patrons and who is authorized to access other patron's data
- Verification process for releasing patron data to a patron or an authorized patron
- Staff processing of patron data, including collection, storage, and retention
- Incident response, including unauthorized access or release of patron data by third parties
- Data sharing with third parties, including vendors and external departments

Implementing procedures follows a similar path with implementing policies: clear communication to staff, accessible documentation, and review schedules. An additional action you should consider taking is creating talking points or a script for your staff to use when they receive questions from patrons regarding privacy at the library. Having language or scripts for staff makes sure that staff are able to provide consistent messaging about privacy to the public.

CONSIDERATIONS

Procedures, like policies, are written for a specific audience in mind, which could be a department or project group. You also need to consider the format of the procedure in relation to how that procedure will be used. A lengthy procedure written in long-form is most likely not going to help staff at the front desk who need to address an issue now. What will help them is a document that is easy to follow: a numbered list, bullet points, short sections, or a visual

diagram. These formats lend themselves to more efficient processing of procedure information on short notice.

Writing a procedure to account for all edge cases leads to an unwieldy document for your staff. Guidelines can exist alongside procedures. While guidelines are less prescriptive than procedures, they help library workers by providing parameters in which to operate in and other considerations, allowing staff to use their best judgement.

Practice

Practice is what happens when you try to implement policy and procedure in daily operations. Practice is subject to several known and unknown factors for both library staff and patrons.

STAFF FACTORS

Communication — Your organizational communication issues can put patron privacy at risk through insufficient training, insufficient documentation, or lack of clear communication lines.

Things outside the library's control — You don't have control over all the situations your staff encounter at the library, nor do you have much control over changes outside the library.

Administration — Administrators set organizational priorities and goals, and have substantial power to make or break effective privacy practices at the library. Examples of administrative decisions affecting privacy practices include funding privacy training and providing agency and resources to staff working on privacy operation planning and implementation at the library.

The human factor — Library staff are trained to provide good customer service. There is often a perception by library workers that providing less than excellent customer service may put their employment in jeopardy. When coupled with the desire to be a helpful citizen and to provide as much assistance as possible when it is requested, this can lead to oversights or missteps in protecting library data and upholding patron privacy, particularly if the data is being requested by other government entities like law enforcement. Training and role playing with staff on how to respond to privacy scenarios before they occur could help eliminate some of the human factor.

PATRON FACTORS

Information overload — Research confirmed what we already know – users don't read all the notices they encounter, and click past through them without reading what was on the screen. The library's privacy practices should reflect the reality that patrons are overwhelmed and might not have the resources to effectively protect their privacy at the library.

Patron expectations — Patrons use the library with a set of expectations about their level of privacy. While some data collection, use, and sharing are part of business operations, your library also collects patron data that is non-essential for library operations. Some libraries combine patron data with external data that the patron did not disclose with the library. In both cases, what recourse does the patron have? Any

non-essential data collection, processing, and sharing needs to address how patrons can exercise their data privacy rights at the library to not have their data included in these processes.

Increased surveillance and privacy risks for some patrons — several patron populations are under significant surveillance from both the government and from the private sector. These patrons face the reality of systems that discriminate against them in various institutions, such as the criminal justice, health care, and education systems, as well as employment processes and credit and housing applications. Several of our patron populations distrust public institutions such as the library if they are tied to a government agency because of fears of data sharing with the government. In these cases, the library needs to cultivate relationships with community groups and organizations that represent these patron groups as a first step to address those realities. The library should work with these groups to ensure that library privacy practices address the possible harms from those practices.

Training Library Staff

Your library privacy policies and procedures are only as effective as the person with the least amount of knowledge and experience with them. How can you create a training program that is not only informative but useful for your staff?

- Create interactive, scenario-based trainings to provide staff context needed to understand and implement policy and procedure
- Provide opportunities for staff to discuss privacy-related issues in training sessions as well as asynchronous discussions in electronic staff forums or discussion lists
- Have a regular training schedule for new staff as well as refresher trainings for existing staff
- Update training materials regularly
- Have training materials readably accessible to staff through the staff intranet or knowledge base

Libraries should also explore training and discussion opportunities surrounding privacy needs and issues around key patron communities. In regards to digital literacy and information privacy and security topics, consider a "train-the-trainer" model for staff who work with patrons so staff have the tools and knowledge needed to teach patrons about those topics.

SECTION 5

VENDORS AND PRIVACY

Please visit https://plpinfo.org/dataprivacy for training materials, resources, and template files referenced in this section.

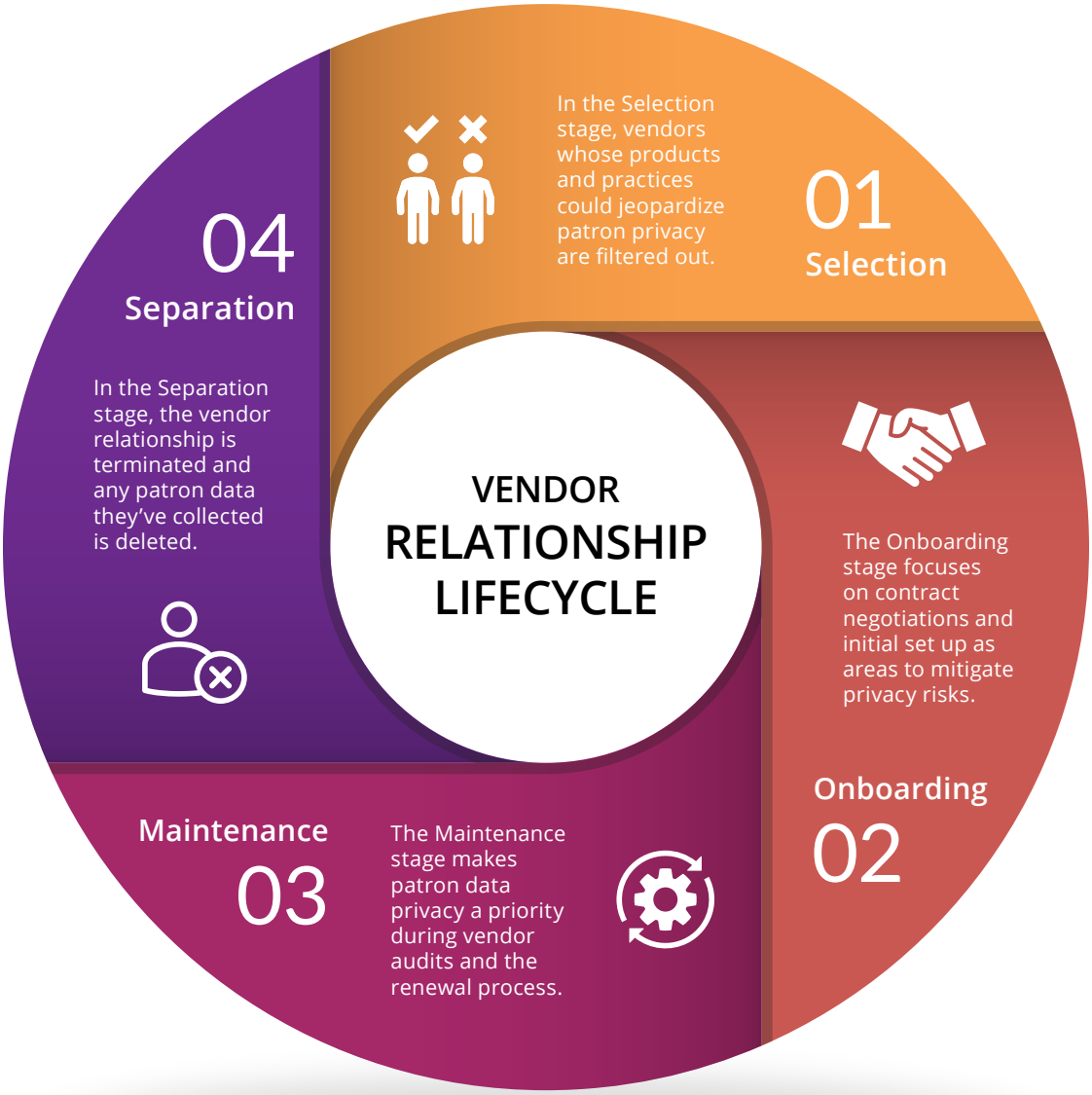
Libraries rely on vendors to handle core and other critical services for the library. We can use the data lifecycle to identify key risks presented by vendor services, but that's only the start. Like operationalizing privacy at your library, working with vendors to protect privacy requires a systematic approach.

Vendor Relationship Lifecycle

The vendor relationship cycle can help your library identify and mitigate privacy risks while working with vendors. The cycle starts with the selection process, then working with the vendor, and then the eventual end of the business relationship. Each stage of the lifecycle provides opportunities to mitigate patron privacy risks.

Some libraries do not have control over a stage and must go through an external department or organization. The best-case scenario is to cultivate the relationship between the library and the external department so they have a better understanding about the importance of library data privacy to better advocate for the library when dealing with vendor-library issues. Even if you are working with a library consortium, it's still worthwhile to build that relationship between your organizations if your library has specific needs or concerns that other libraries in the consortium might not have.

Vendor Relationship Lifecycle



Selection

IDENTIFYING VENDORS WHO PRIORITIZE PRIVACY

The selection process is where the library has the most control over in the vendor relationship lifecycle. This stage gives you the chance to filter out vendors whose products and practices could put patron privacy at risk.

Tools and best practices — RFI and RFP

Request for Information (RFI) — This is the fact-finding part of the selection process. RFIs can give you a general sense as to the privacy practices and features of these services and products.

Request for Proposals (RFP) — RFPs are when you are ready to collect bids from vendors for a specific product or service. At this stage you can get more details regarding privacy, from requiring the vendor to report on certain information to outlining privacy requirements for the product or service.

RFPS AND FUNCTIONAL REQUIREMENTS

RFP templates typically contain boilerplate language around several requirements, and you can also take this approach to create a template of privacy and security functional requirements. Requirements can be **prescriptive** ("Service/product must…") or **descriptive** ("Explain how the service/product…").

Prescriptive requirements work best when you can provide a detailed, comprehensive list of privacy and security requirements for the product or service. Prescriptive requirements make it clear at the start to vendors about what you expect, but this approach does not allow vendors to elaborate on their answers to the requirements.

Descriptive requirements allow the vendor to explain in detail how they meet the specific requirement. This approach lets libraries find out how vendors approach privacy without having to compile a comprehensive list, which can be time consuming and prone to missing a key privacy risk. At the same time, the library might have to spend more time with vendors who don't provide enough detail in their initial answers.

At minimum, your functional requirements should cover the following privacy and security items:

Privacy features and requirements

- Vendor conducting regular security and privacy audits
- Ability for patrons to opt-in/opt-out of non-essential data collection at any time
- Library and patron ability to control disclosing patron data to subcontractors, service providers, and other third parties.
- Library ability to change data retention settings
- Vendor must have privacy policy on record
- Vendor compliance to local, state, and relevant federal regulations

- Library and patron ability to export and delete data at time of separation

Security features and requirements

- Physical and electronic access controls in place to restrict access to patron data to only those who need access to perform a core business function
- Encryption of patron data at rest and in transit using current industry standards considered secured at the time of the RFP
- Secure media destruction of both electronic data and the physical formats and media that stored patron data
- Industry standards, principles, or certifications, such as International Organization for Standardization (ISO) certifications, or NIST guidelines for data privacy and media sanitation

Onboarding

CLARIFYING EXPECTATIONS TO MITIGATE RISK

In this stage we'll focus on contract negotiations and initial set up as areas where we can mitigate privacy risks.

Contract negotiation

Contract negotiations are essential in protecting the privacy of your patron data, but you have multiple sides who all want their own interests written into the contract. Knowing what features and requirements your library is willing to push for, willing to negotiate a compromise on, and willing to leave the talks and start the selection process over before the negotiations start will provide much needed guidance for library staff and reduce the chance of signing onto a contract that puts patron privacy at risk.

LEGAL REGULATIONS

Any contract should be reviewed by legal counsel during the negotiation process. We'll focus on state law, again with the recommendation to work with legal staff regarding compliance with these and other federal, state, and local regulations.

California Government Code Section 6267 states that any library who receives public funding shall keep patron use records confidential. This section does not only address libraries, but others that store or otherwise maintain patron use records on behalf of the library. Vendors who collect or store patron data most likely need to comply with section 6267.

Your vendor might also need to comply with *the California Consumer Privacy Act of 2018 (CCPA).* There are two areas that libraries should be aware of as their vendors work on CCPA compliance:

- Businesses can pass information from person along to another person requesting their personal information if the business determines that they are part of a single household. This could compromise privacy if information about a patron's activities is provided to another patron.
- CCPA requires businesses to get affirmative consent from 13 to 16-year old persons before selling their personal data. This might mean that your vendor will be collecting additional patron information.

One more state law to keep in mind is *California Civil Code Section 1798.82* surrounding data breaches and incident response. This section defines personal information and coordination of who is responsible for what, including timelines for written or electronic notice to those involved in the breach. You can find a notice template at http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.82.

OTHER AREAS OF NEGOTIATION

- **Privacy policy —** You can include in the contract that the vendor must comply with the library's privacy policy.
- **Vendor data security and privacy requirements —** Include industry standards, like PCI or ISO standards, where appropriate.
- **Patron control over collection of non-essential data collection —** By default, all non-essential data collection should be turned off by default, and the patron should be able to turn on and off this collection at any time.
- **Data deletion at end of business relationship —** patron data must be deleted by the vendor when the business relationship ends.

CONTRACT RED FLAGS

There are many red flags that can turn up in a contract. Here are a few major red flags that can appear in a vendor contract:

- Use of the word "reasonable" and other vague terms
- Lack of definitions for terms such as "data," "user," "measures of protection," etc.
- Indemnity/liability clauses which hold the vendor harmless if something goes wrong
- Lack of details regarding what will happen during termination of contract
- Lack of information about responses to law enforcement or government data requests
- Legal jurisdiction of the contract different than your legal jurisdiction
- Lack of overall transparency
- Data ownership – who owns the data: the library, patron, or the vendor?
- Data reselling or disclosure to other third parties
- Monitoring patron use, including web analytics
- Referring to privacy policies or terms of use outside of the contract that are subject to change without notice and without revision of the contract when changed
- Using "Aggregated," "Anonymized," "De-identified" without defining methods

TOOLS — CONTRACT ADDENDUMS AND NON-DISCLOSURE AGREEMENT

To help speed along the negotiation planning process on your end and to ensure that you don't miss a key negotiation area, use **contract addendums** and **non-disclosure agreement (NDAs).**

Contract addendums are your boilerplate for privacy and security language and requirements. Once vetted by legal counsel, you can use this document in both initial contract signings as well as renewing existing contracts. Libraries approach contract addendums in several ways, including adding line items in the main contract text, or attaching them as appendixes to the contract.

NDAs limit or prohibit the vendor from sharing patron data under most circumstances to third parties. NDAs are

narrow in scope. Contract addendums are more comprehensive in terms of detailing privacy requirements. Some libraries choose to integrate NDA language into their contract addendums, while others keep the documents separate.

Setting up the service and data importing

Never accept data collection, storage, sharing, or retention defaults without first reviewing each setting. For some services you can control what type of data collected, including services that provide options for user input, to avoid the vendor collecting non-essential data points from patrons.

Your vendor most likely uses Google Analytics, which collects patron data every time they visit a site. Ask your vendor to turn off tracking or use another tracking software that is more privacy-oriented or minimizing the identifiable data being collected by Google Analytics.

The vendor might ask you to upload patron data to them before implementing the service. **Just because there is a spot for a data point doesn't mean that the service absolutely needs that data.** Before uploading the data, assess the risk associated with uploading patron data. Sometimes the data requested by the vendor doesn't fit into the needs you have for that service.

Maintenance

REVIEWING VENDOR CONTRACT AND ENFORCING TERMS

In the maintenance stage, libraries need to keep privacy a priority, including in vendor audits and the renewal process.

Vendor audits

Vendor audits serve as the periodic review of vendor privacy practices during the business relationship. Work with the vendor on the "what, where, when, and how" of the audit, including any industry standards or checklists to work with, when audits are done, and the process for addressing areas of improvement or risk.

Some libraries choose to conduct vendor security and privacy audits on their own. These audits are limited to what the library can access; however, libraries can conduct audits on specific features or functions, such as assessing the protection of patron data on vendor websites, to assess the privacy and security practices of the vendor.

Other libraries require vendors to perform comprehensive security and privacy audits on a yearly basis. The audit might be a questionnaire created by the library or an existing questionnaire from another organization to ensure contractual obligations and security industry standards are met. A weakness of this approach is vendor self-reporting. One way to address this weakness is to bring in an independent party to perform the audit on the vendor. This approach will require negotiations with the vendor in the choice of the auditor, as well as the cost and planning in bringing the auditor into the process.

Renewals — to renegotiate or to leave

The renewal process is an opportunity for both vendors and libraries to renegotiate contract terms and expectations. Libraries can add addendums at this time if there isn't already one attached to the contract.

It is possible to renegotiate terms, but there is also the reality of needing to leave a vendor if their privacy practices put patrons at risk and the vendor refuses to negotiate. Sometimes when enough libraries do not renew with a vendor who implemented a change that puts privacy at risk, the vendor is more willing to rescind the change, as it was the case with LinkedIn Learning's rescinding of authentication changes in early 2020 that would have put patron privacy at risk.

Separation

REMOVAL OF ACCESS TO YOUR PATRON DATA

Having proper selection, onboarding, and maintenance procedures in place ensures that when you arrive at the point of separation, removal of vendor access to your patron data runs smoothly.

Ending a vendor relationship is a complicated and stressful process. There are a couple of strategies to make the process less risky to patron privacy, but this work must happen long before the separation:

- **Selection —** add functional requirements about exporting and deletion of patron data after termination of business relationship
- **Onboarding —** add requirement in contract or addendum to export and delete patron data at time of termination of business relationship
- **Maintenance —** conduct privacy audits to catch patron data retained longer than it needs to be for operational purposes

At the end of the business relationship, work with the vendor to export and delete patron data, including any data that might be living in vendor backups or archived logs. Vendors also need to work with their subcontractors or other third parties to delete any patron data shared with these parties.

Communicating About Vendor Privacy Practices

The same communication issues and strategies discussed in previous sections apply to the library's use of vendors. In Section 4 we discussed vendor privacy policy pages to provide a central place for patrons and staff to view all the available privacy policies of the vendors the library uses.

Internal announcements to staff through email, staff intranet, or meetings are one way to make sure that your staff is prepared for patron questions patrons. You should also doublecheck to ensure that the product or service follows existing library privacy policies.

You might already be planning public announcements about the new vendor or service to your patrons, so now would also be a good time to add the public privacy notice from the vendor to the vendor privacy policy page. Like our internal privacy policies, doublecheck to make sure that the product or service matches what you are telling your patrons in your public privacy notice.

Sometimes there are vendors that will not change certain settings to protect patron privacy by default, such as a vendor not turning off borrowing history by default. "Just-in-time" notices and alerts on the vendor sign in page can alert patrons of this setting and give them instructions to change this setting if they so choose.

SECTION 6

SPECIAL PRIVACY TOPICS

Please visit https://plpinfo.org/dataprivacy for training materials, resources, and template files referenced in this section.

This section covers several topics that are of special importance to protecting patron privacy but require additional explanation and consideration.

Law Enforcement Requests

Libraries must have policies and procedures in place surrounding law enforcement requests for patron data. All staff must receive regular training on and have access to quick guides to these procedures for staff to use at the point of request. ALA has extensive guidelines that can help libraries create policies and procedures. Additionally libraries should consider talking to legal staff in finalizing the documents.

California Government Code Section 6267 protects patron use records from disclosure except for a few cases, such as a court-issued order. ***Administrative warrants*** are not ***judicial warrants*** — judicial warrants are issued from a court judge, while administrative warrants are not. Administrative warrants do not fall under the court order exception for disclosure of patron data in the section. Staff should also not give officers information about a patron unless there is a valid court-issued order. The officers can go into public spaces such as the library to ask individual patrons questions, but the library should have a court-issued order before releasing any information.

Vendors who fall under Section 6267 must also protect data from disclosure to law enforcement unless there is a valid court order. During the Selection stage, ask vendors about their data disclosure policies including disclosures to law enforcement. Your contract addendum should also address the conditions when data should be disclosed to third parties, such as law enforcement.

Patron Access to Other Patrons' Records

Patron records should not be disclosed to other patrons except when there is written consent from the patron, as stated in Government Code Section 6267. Libraries can create policies and procedures that allow patrons to access other patron's information — including adult custodians, parents, and legal guardians — but libraries must ensure that these policies and procedures fall within state and local regulations.

Libraries who wish to offer an authorized patron option at their library should consider the following:

- Limit access to what is absolutely necessary. For example, if the primary goal is to allow other patrons to pick up holds for another patron, then the patrons do not need to have access to the patron's borrowing history or other information in the record to check out the hold item.
  - In some cases, there will be a need for additional access to patron information. For example, case workers might request specific access to clients' patron record, such as fees or fines. Libraries should work with legal staff as well as the agencies of the case workers in drafting a specialized authorized access procedure.
- The patron must have the option to revoke access of any authorized patrons at any time.
- Create a verification process to ensure the identity of the authorized patron. This could include confirmation of two data points in the record of the authorized patron, including address and age.
- There should be a note in both the patron and authorized patron records that indicate that the patron has authorized the other patron to access their information.

Section 6267 does not provide an exception for parental or legal guardian access to their child's record. Public libraries who create policies around parent or guardian access to another patron's records must address when a minor or adult ward obtains the same level of privacy as adult patrons. Some libraries give this right when patrons turn 18, while other libraries give this right to 13 year olds as "mature minors" (for more information about the legal standing of the constitutional rights of 13-17 year olds, read https://scholarship.law.upenn.edu/jcl/vol2/iss1/9). School libraries should be aware that library records are usually considered educational records and are subject to FERPA disclosure requirements.

Library vendors who need to comply with CCPA introduce another potential release of patron data to other patrons through CCPA's inclusion of household data as data that can potentially be released to a consumer requesting a copy of their data. Libraries should talk to vendors about how they are determining households in data requests. Libraries should also talk to patrons about how the data rights granted to them by CCPA could affect their privacy while using third-party products at the library.

Security at The Library

Under Government Code Section 6267, "patron use records" includes written or electronic records that contain information that could be used to identify the patron, like a name or email address, as well as any record or transaction that identifies a patron's use of the library. This includes online use such as search histories, research chat transcripts, and electronic resource search records and activity. This is a broad definition which leaves room for interpretation, particularly around security at the library.

Incident tracker systems and shift logs are two places where patron information is collected, stored, and retained. These applications could be subject to public

records requests, depending on your local regulations, but they could also be protected under Section 6267. Legal staff can assist in determining what is protected and what is subject to disclosure in these areas.

Another gray area is the use of security cameras in libraries. ALA recommends that library policies around security camera should include providing physical notices to patrons about the use of cameras, secured storage of the recordings, and the destruction of the recordings when permitted by law, or after the recording's purpose has been served. The policy should state that the cameras are there solely for the purpose of enhancing physical security of the library as well as the people working and using the library.

Security camera recordings may or may not be considered a patron use record, depending on several factors:

- **Placement of the cameras —** How you position the camera could minimize the risk of capturing use of specific library resources, such as not placing a camera that records use of the stacks or what is on the screen of a public computer. At the same time, some of the highest trafficked areas, such as the circulation and information desks and the public computing areas, will contain uses of specific library materials.
- **Overall management of cameras —** Sometimes the security cameras are implemented and maintained by another organization or department outside of the library. Depending on what the recording captures, as well as the relationship between the library and the outside department, there might be a case that the outside department falls under Section 6267 and is subject to the same requirements of keeping patron use records confidential. ***Libraries who contract with law enforcement in maintaining in building security cameras should reconsider the arrangement and investigate alternative arrangements to contract with for security camera management.***

Marketing, Fundraising, and Data Analytics

Libraries are increasing using patron data for marketing and fundraising purposes with either local databases of patron information or through using customer relationship management systems (CRMS). In practice, it is considerably difficult to use patron data for marketing or analysis while operating within privacy policies, patron expectations, and professional ethics.

De-identification limitations and re-identification risks

Some libraries might consider de-identification of patron data to protect patron privacy. However, de-identification is not fool-proof as described in Section 2. Anonymization, which breaks the data points from any individual, is near impossible to achieve and still carries the risk of re-identification. Vendors who advertise or claim to de-identify or anonymize patron data should be asked about their methods as well as how they calculate the risk of re-identification of the data.

Patron expectations and data ethics

There are certain types of data that patrons do not expect libraries to collect. For example, patrons do not give income and education data to the library as part of the library registration process; therefore, there is a level of expectation that the library would not have this data. However, market segmentation and other forms of data analyses pull in this type of data from third party sources using existing patron data. This is of concern for libraries using third party CRMSs where the vendor might also disclose patron data in the process, as well as retain the ownership of any patron data you input into the system, even when you end the business relationship.

If your patron's reaction to your data practices is "you did *what* with my data?," you have a violation of expectations, as well as a possible *ethics breach. Ethics breaches* are the failure to handle data consistent with organizational or professional values. If a library privacy notice doesn't mention market segmentation or use of third party data to create user profiles, then patrons will assume that the library will not be engaging in these practices. When these practices become public knowledge it can lead to a loss of trust of and a damaged relationship with the library. One publicized case was Santa Cruz Public Library and the Civil Grand Jury investigation into the library's use of Gale's Analytics on Demand in 2019.

Any type of data processing for marketing, fundraising, and analysis will require a high level of transparency and openness with your patrons about your data practices to mitigate violated patron expectations. At minimum, using the library privacy notice to inform patrons about how data is used at the library for profile and marketing – as well as creating a process in which they can control how their data is used and shared by the library – can help mitigate expectation violations.

Data analytics, equity, and privacy — a balancing act

Before starting a market segmentation project, or other types of targeted marketing analysis, libraries must carefully consider the reasons for engaging in these types of patron data processing. Data analysis is a powerful tool to inform decision making at the library, but it must not be the only tool used to make decisions. Data collection can miss critical context about part of the service population, and processing can be easily influenced by several human biases and factors. Several patron communities face discrimination and disadvantages in many systems and organizations due to algorithms and models based on bad data collection and processing. The same types algorithms and models exist in many library applications and systems. Libraries who solely rely on data to inform the library's relationship with the community run the risk of replicating those same discriminatory practices found in other systems and structures in society.

Relying on market segmentation or data analysis can lead to missed opportunities to better serve underserved or unserved patron communities since these activities

focus on library patrons who already use library services that collect patron data. Data analysis can indicate certain gaps in service in certain locations or patron populations, but the library's next action should be to add qualitative data to provide context to the data. This includes facilitating community listening sessions that include different patron communities and building working relationships with community groups and organizations. Taking the time and resources to build these relationships is an investment in protecting patron privacy by not defaulting to more invasive practices of creating a profile of the patron's use of the library that is vulnerable to data breaches or leaks if a library chooses to use analytical tools, library administration and staff should discuss together how the tool will be used, what data will be gathered and shared, and how the information will be stored and used, so that there is a clear understanding internally of proper handling of data.

Public Computing

Protecting patron privacy includes securing the technological infrastructure of the library through information security standards and best practices. There are several resources about how to secure a library's technological infrastructure at https://plpinfo.org/dataprivacy, but here are some key practices to protect patrons using the infrastructure:

Library website

- Encrypt all traffic on the library website using HTTPS

Network and Wi-Fi

- Route internet traffic from public computers in a different subnet from other library subnets so that networks remain separate in case of a cybersecurity attack or other type of breach
- Configure network traffic to not be able to trace one IP address to an individual public computer by using DHCP or other means
- Configure the firewall to block ads, spam, and malware and consider blocking file sharing
- Allow VPN use on the library Wi-Fi
- Inform patrons of any potential privacy and security risks in using the library Wi-Fi. This can be done by requiring acceptance of the library's computer use policy before granting Wi-Fi access.

Public computers

- Install privacy-oriented browsers, such as Brave, Firefox, and Tor on the desktop image
- Install privacy-oriented browser addons that block ads, web script, and trackers
- Install anti-virus and anti-malware software on the desktop image
- Do not track patron activity during the session, including website visits and search activity
- Purge all downloaded files, caches, or other data from the session once the session has either timed out or ended by the patron

- Provide privacy screens for all public computers
- Purge computer reservation logs of any identifying patron information at the end of each day

Printers, scanners, and copier machines

- Wipe the memory or drives daily and before the machine ends its service at the library

Risk Assessment

Library-wide risk assessment requires the adoption of many processes and policies to gain a better understanding of the overall risks to patron privacy, as well as how the library can address those risks. The previous sections explored specific tools and frameworks to identify and mitigate specific risks, such as the patron data and vendor relationship lifecycles, privacy impact assessments, and data inventories.

Risk assessments cover any process that handles patron data, not just data in a database or application. This includes processes that are a mix of technical and non-technical components: for example, the collection of personal data on paper then transferring that data into a spreadsheet, or exporting data from a system into a physical format to deliver to another person.

General risk assessment includes:

- Identifying the type of data collected and processed by the library and third-parties contracted by the library into risk categories such as:
  - **High risk —** data that is most likely to cause harm to both patrons and the library if breached or leaked
  - **Medium risk —** data that can cause harm if leaked or breached when combined with at least one other data point
  - **Low risk—** non-personally identifying data
- Assessing the types of privacy risks present in libraries and third-party vendors, including determining the likelihood and severity of each risk
- Determining how the library will address each risk: acceptance, transference, mitigation, or elimination
- Developing processes to regularly reassess privacy risks and risk reduction strategies

Libraries interested in learning more about library data risk assessment processes should consult *"A Practical Guide to Performing a Library User Data Risk Assessment in Library-Built Systems"* published by the Digital Library Federation (DLF) – http://doi.org/10.17605/OSF.IO/V2C3M.

SECTION 7

LIBRARY PRIVACY RESOURCES

Acronyms

ALA	American Library Association
BYOD	Bring Your Own Device
CalOPPA	California Online Privacy Protection Act of 2003
CCPA	California Consumer Privacy Act
CLA	California Library Association
COPPA	Children's Online Privacy Protection Act
Data FOMO	Data Fear Of Missing Out
FERPA	Family Educational Rights and Privacy Act
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
HTTPS	Hypertext Transfer Protocol Secure
IANAL	I Am Not A Lawyer (always a good acronym to have in your pocket!)
IFLA	International Federation of Library Associations and Institutions
ILS	Integrated Library System
ISO	International Organization for Standardization
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
OECD	Organisation for Economic Co-operation and Development
PbD	Privacy by Design
PII	Personally Identifiable Information
RFI	Request For Information
RFP	Request For Proposals

Data Privacy Terminology

Cost
The potential impact on the target by a threat, be it financial, reputational, legal, operational, or other types of impact on both the organization and the people targeted by the threat.

Data Privacy
Actions around the appropriate handling, controlling, sharing, and disposal of personal data assets.

Information Security
Actions that protect personal and non-personal data assets.

Risk
The potential cost resulting from a threat taking advantage of a vulnerability.

Threat
A potential scenario that can cause damage or loss to an organizational asset.

- ***Related term — threat actor:*** Someone or something that could be responsible for creating said harm to the organization. Threat actors can act out of malicious intent, but can also exploit a vulnerability even if there is no malicious intent.

Vulnerability
A weakness in any system or structure that a threat can use to cause harm to the organization. Vulnerabilities can be either technical and non-technical in nature.

Professional Standards and Guidelines

America Library Association (ALA)

Library Bill of Rights. http://www.ala.org/advocacy/intfreedom/librarybill.

Library Privacy Checklists. http://www.ala.org/advocacy/privacy/checklists.

Library Privacy Guidelines. http://www.ala.org/advocacy/privacy/guidelines.

Questions and Answers on Privacy and Confidentiality. http://www.ala.org/advocacy/privacy/FAQ.

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

Privacy. http://www.ala.org/advocacy/privacy.

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

Privacy Tool Kit. http://www.ala.org/advocacy/privacy/toolkit.

Professional Ethics. http://www.ala.org/tools/ethics.

Resolution on the Retention of Library Usage Records. http://www.ala.org/Template.cfm?Section=ifresolutions&Template=/ContentManagement/ContentDisplay.cfm&ContentID=135888.

State Privacy Laws Regarding Library Records. http://www.ala.org/advocacy/privacy/statelaws.

Students & Minors. https://chooseprivacyweek.org/resources/students-and-minors/.

Suggested Guidelines: How to Respond to Law Enforcement Requests for Library Records and User Information. http://www.ala.org/advocacy/privacy/lawenforcement/guidelines.

Video Surveillance in the Library Guidelines. http://www.ala.org/advocacy/privacy/guidelines/videosurveillance.

Digital Library Federation (DLF)

Asher, Andrew, Kristin Briney, Gabriel J. Gardner, Lisa Janicke Hinchliffe, Bethany Nowviskie, Dorothea Salo, and Yasmeen Shorish. 2018. "Ethics in Research Use of Library Patron Data: Glossary and Explainer." DLF Privacy and Ethics in Technology Working Group. https://doi.org/10.17605/OSF.IO/XFKZ6.

Bettinger, Eliza, Mahrya Burnett, Michelle Gibeault, Yasmeen Shorish, and Paige Walker. 2019. "Advocacy Action Plan." DLF Privacy and Ethics in Technology Working Group. https://doi.org/10.17605/OSF.IO/J5K8S.

Briney, Kristin, Becky Yoose, John Mark Ockerbloom, and Shea Swauger. 2020. "A Practical Guide to Performing a Library User Data Risk Assessment in Library-Built Systems." DLF Privacy and Ethics in Technology Working Group. https://doi.org/10.17605/OSF.IO/V2C3M.

Walker, Paige, Jen Ferguson, Chelcie Juliet Rowell, Yasmeen Shorish, Eliza Bettinger, and Brandon Patterson. 2020. "Digital Privacy Instruction Curriculum." DLF Privacy and Ethics in Technology Working Group. https://doi.org/10.17605/OSF.IO/SEBHF.

International Federation of Library Associations and Intitutions (IFLA)

IFLA Code of Ethics for Librarians and Other Information Workers. https://www.ifla.org/publications/node/11092?og=30.

IFLA Statement on Privacy in the Library Environment. https://www.ifla.org/publications/node/10056.

Internal Organization for Standardization (ISO)

ISO/IEC 27001 - Information Technology – Security techniques – Information security management systems – Requirements

ISO/IEC 27701 - Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

Legal Regulations

International

Berman, Erin. 2018. "GDPR and American Public Libraries." Public Libraries Online. http://publiclibrariesonline.org/2018/06/gdpr-and-american-public-libraries/.

Heller, Margaret. 2018. "Introducing Our New Best Friend, GDPR." ACRL TechConnect. https://acrl.ala.org/techconnect/post/introducing-our-new-best-friend-gdpr/.

Kulesova, Katya. 2019. "Is Your Company Subject to the GDPR? Consider These 5 Factors." https://iapp.org/news/a/is-your-company-subject-to-the-gdpr-consider-these-5-factors/.

Wittmaier, Nathan. 2019. "GDPR for American Public Libraries." https://2019.code4lib.org/talks/GDPR-for-American-Public-Libraries.

Federal

"Complying with COPPA: Frequently Asked Questions." Federal Trade Commission. https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

"Protecting Student Privacy." U.S. Department of Education. https://studentprivacy.ed.gov/?src=fpco.

California state law

California Civil Code § 1798 Title 1.81 Customer Records. http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.&part=4.&chapter&article=

California Consumer Privacy Act of 2018 (CCPA). https://www.oag.ca.gov/privacy/ccpa.

California Government Code § 6254. Records Exempt from Disclosure Requirements. https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=6254.&lawCode=GOV

California Government Code § 6267. Registration and Circulation Records of Library Supported by Public Funds. https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=6267.&lawCode=GOV

California Online Privacy Protection Act of 2003 (CalOPPA). https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=8.&chapter=22.&lawCode=BPC.

California State Library. 2019. "California Library Laws." https://www.library.ca.gov/services/to-libraries/library-laws/.

Industry Standards and Best Practices

Cavoukian, Ann. 2011. "Privacy by Design: The 7 Foundational Principles." Information and Privacy Commissioner of Ontario. https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

Federal Trade Commission. 2009. "Fair Information Practice Principles." Archived at https://web.archive.org/web/20090331134113/http://www.ftc.gov/reports/privacy3/fairinfo.shtm.

Garfinkel, Simson L. 2015. "De-Identification of Personal Information." NIST Interagency/Internal Report (NISTIR) - 8053. National Institute of Standards and Technology. https://www.nist.gov/publications/de-identification-personal-information.

Kissel, Richard, Andrew Regenscheid, Matthew Scholl, and Kevin Stine. 2014. "Guidelines for Media Sanitization." NIST SP 800-88r1. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-88r1.

McCallister, E, T Grance, and K A Scarfone. 2010. "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)." NIST SP 800-122. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-122.

NIST. 2017. "Section 8 - Privacy Considerations." NIST SP 800-63. National Institute of Standards and Technology. https://pages.nist.gov/800-63-3/sp800-63a/sec8_privacy.html#genProofReqs.

NIST. 2018. "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1." NIST CSWP 04162018. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018.

NIST. 2020. "NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management". Version 1.0. https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf.

OECD. 2013. "OECD Privacy Guidelines." OECD. http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm.

PCI Security Standards Council Site. https://www.pcisecuritystandards.org/.

SANS Institute. 2013. "20 Critical Security Controls." Archived at https://web.archive.org/web/20131101135802/http://www.sans.org/critical-security-controls/spring-2013-poster.pdf.

De-identification and Re-identification

Armoza, Jonathan. 2014. "Riding with the Stars: Passenger Privacy in the NYC Taxicab Dataset." September 15, 2014. https://research.neustar.biz/2014/09/15/riding-with-the-stars-passenger-privacy-in-the-nyc-taxicab-dataset/.

Barbaro, Michael, and Tom Zeller Jr. 2006. "A Face Is Exposed for AOL Searcher No. 4417749." The New York Times, August 9, 2006. https://www.nytimes.com/2006/08/09/technology/09aol.html.

Bettilyon, Tyler Elliot. 2019. "Why 'Anonymized Data' Isn't So Anonymous." OneZero. April 24, 2019. https://onezero.medium.com/why-anonymized-data-isn-t-so-anonymous-535d2db75a2d.

Lubarsky, Boris. 2017. "Re-Identification of 'Anonymized' Data." Georgetown Law Technology Review. April 12, 2017. https://georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/.

Polonetsky, Jules, Omer Tene, and Kelsey Finch. 2016. "Shades of Gray: Seeing the Full Spectrum of Practical Data De-Identification." Santa Clara L. Rev. 56: 593.

Vendor Assessment Tools

Caro, Alex and Chris Markman. 2016. "Measuring Library Vendor Cyber Security: Seven Easy Questions Every Librarian Can Ask." The Code4Lib Journal. https://journal.code4lib.org/articles/11413.

Coyle, Karen. "Library Privacy Audits." http://www.kcoyle.net/privacy_audit.html.

"Higher Education Community Vendor Assessment Toolkit." EDUCAUSE. https://library.educause.edu/resources/2016/10/higher-education-community-vendor-assessment-toolkit.

Information Security Office. "Details of the Vendor Security Assessment Program." University of California Berkeley. https://security.berkeley.edu/services/vendor-security-assessment-program/details-vendor-security-assessment-program.

Quintin, Cooper, and Soraya Okuda. 2018. "How to Assess a Vendor's Data Security." Electronic Freedom Foundation. January 8, 2018. https://www.eff.org/deeplinks/2018/01/how-assess-vendors-data-security.

"SJPL Vendor Security Analysis." San Jose Public Library. https://drive.google.com/drive/folders/1jdPwQeC5RAUbBWLAhylYxWHa0pTdVObc

"Vendor Security Assessment Questionnaire." Santa Cruz Public Library. https://www.santacruzpl.org/files/data_privacy/docs/SCPLVendorSecurityAssessmentQuestions.pdf.

Negotiation Resources

Berdzeni, Natalya. 2016. "Negotiation tips for library directors." LAC Group. February 22 2016. Accessed September 6, 2019. https://lac-group.com/negotiation-tips-library-professionals/.

Boss, Richard W. n.d. "Negotiating Contracts with Integrated Library System Vendors." PLA Tech Notes. https://alair.ala.org/bitstream/handle/11213/258/Negotiating%20with%20ILS%20Vendors.pdf?sequence=99&isAllowed=y.

Dygert, Claire T., and Elizabeth Parang. 2013. "Honing Your Negotiation Skills." The Serials Librarian 64 (1–4): 105–10. https://doi.org/10.1080/0361526X.2013.760395.

Gruenberg, Michael. 2015. "Both Sides Now: Vendors and Librarians - Managing the Negotiation Process with Library Vendors." Against the Grain. Accessed September 6, 2019. https://www.against-the-grain.com/wp-content/uploads/2015/03/both_sides_now_v26-6.pdf.

Marsh, P. D. V. 2001. Contract Negotiation Handbook. Gower Publishing, Ltd.

Smith, Jane, and Eric Hartnett. 2015. "The Licensing Lifecycle: From Negotiation to Compliance." The Serials Librarian 68 (1–4): 205–14. https://doi.org/10.1080/0361526X.2015.1017707.

Stroshane, Eric. 2017. "Negotiating Contracts with Vendors for Privacy." Intellectual Freedom Blog. May 3, 2017. Accessed September 6, 2019. https://www.oif.ala.org/oif/?p=9578.

PLP Data Privacy Best Practices Trainings

The following trainings were developed for the LSTA funded D*ata Privacy Best Practices Training for Libraries project,* held in person and online in early 2020. To access the resources listed in this section, go to plpinfo.org/dataprivacytoolkit.

Protecting Privacy in the Library Patron Data Lifecycle

Training slides

Workshop handout

EXAMPLES AND TEMPLATES

Data Inventory spreadsheet

Privacy Impact Assessment (PIA) template files:

- Threshold analysis
- Data analysis
- Risk assessment report

Operationalizing Library Privacy: Policies, Procedures, and Practice

Training slides

Workshop handout (includes annotated bibliography of example privacy notices and policies)

Library Privacy and Vendor Management I: A Privacy Oriented Overview of The Vendor Relationship Lifecycle

Training slides

Workshop handout

Library Privacy and Vendor Management II: Exploring Practical Strategies and Best Practices

Training slides

Workshop handout

EXAMPLES AND TEMPLATES

Annotated RFP examples

Annotated contract addendum examples

Other Library Privacy Trainings, Programs, and Courses

Chicago DigitalLearn. https://chipublib.digitallearn.org/ - in particular, check out the "Being Safe Online" section as an example of embedding data privacy into digital literacy and skills programming

Data Privacy Project. https://dataprivacyproject.org/.

Henning, Nicole. "Online Privacy & Security Course." https://nicolehennig.com/courses/privacy-security-best-practices-library-users/.

Library Freedom Institute. https://libraryfreedom.org/index.php/lfi/.

"Main Page/Teaching Resources." Library Freedom Wiki. https://libraryfreedom.wiki/html/public_html/index.php/Main_Page/Teaching_Resources.

NYC Digital Safety. https://nycdigitalsafety.org/.

"Privacy Services." Cornell University Library. https://www.library.cornell.edu/services/privacy.

"Virtual Privacy Lab." San Jose Public Library. https://www.sjpl.org/privacy.

Yoose, Becky. 2020. "Using Privacy Impact Assessments to Protect Patron Privacy." Florida Library Webinars. https://floridalibrarywebinars.org/auto-draft-10/.

Library Privacy Resources

Websites and listservs

Choose Privacy Every Day. https://chooseprivacyeveryday.org/.

Jones, Kyle M. L., Andrew Asher, Kristin Briney, Abigail H. Goben, Michael Perry, Mariana Regalado, Dorothea Salo, and Maura Smale. 2019. "Data Doubles." https://doi.org/10.17605/OSF.IO/D7F3G.

Library Freedom Project. https://libraryfreedom.org/ - in particular, check out the Resources page at https://libraryfreedom.org/index.php/resources/ for staff and patron privacy handouts and training.

SEC4LIB Listserv. http://security4lib.org/mailman/listinfo/sec4lib_security4lib.org.

West, Jessamyn. "Practical Internet Privacy." https://www.librarian.net/talks/privacy/.

Articles and books

AASL. 2006. "Position Statement on the Confidentiality of Library Records." American Association of School Librarians (AASL). http://www.ala.org/aasl/advocacy/resources/statements/library-records.

ALA Office for Intellectual Freedom. 2010. *Privacy and Freedom of Information in 21st-Century Libraries.* Chicago: ALA.

Ayre, Lori Bowen. 2017. "Protecting Patron Privacy: Vendors, Libraries, and Patrons Each Have a Role to Play." *Collaborative Librarianship.* https://digitalcommons.du.edu/cgi/viewcontent.cgi?article=1330&context=collaborativelibrarianship.

Beckstrom, Matthew. 2015. *Protecting Patron Privacy: Safe Practices for Public Computers.* Santa Barbara, California: Libraries Unlimited.

Breeding, Marshall. 2015. *Privacy and Security of Automation and Discovery Products.* https://librarytechnology.org/repository/item.pl?id=20425.

Breeding, Marshall. 2016. *Privacy and Security for Library Systems.* Chicago: ALA TechSource.

Breeding, Marshall. 2019. *Protecting Privacy on Library Websites: Critical Technologies and Implementation Trends.* Chicago: ALA TechSource.

Chmara, Theresa. 2009. *Privacy and Confidentiality Issues: A Guide for Libraries and Their Lawyers.* Chicago: ALA.

Fortier, Alexandre, and Jacquelyn Burkell. 2015. "Hidden Online Surveillance: What Librarians Should Know to Protect Their Own Privacy and That of Their Patrons." Information Technology and Libraries 34 (3): 59–72. https://doi.org/10.6017/ital.v34i3.5495.

Givens, Cherie L. 2015. *Information Privacy Fundamentals for Librarians and Information Professionals.* http://site.ebrary.com/id/10987879.

Hennig, Nicole. 2018. *Privacy and Security Online: Best Practices for Cybersecurity.* Chicago: ALA TechSource.

Hill, Kate, and Tessa Minchew. 2018. "Into the Great Wide Open: Licensing, Vendor Relations, and Data Security During 'Interesting Times'." *Electronic Resources & Libraries 2018.* https://www.dropbox.com/sh/r8yfxwl7h602au6/AABGaKVbMbEg7AnmijmTOApda?dl=0&preview=S079+-+Into+the+Great+Wide+Open+(1).pptx.

Kelly, Robert G. 2013. "Biz of Acq – Negotiating with a Contract Addendum." *Against the Grain* 20 (3). https://doi.org/10.7771/2380-176X.2412.

Kritikos, Katie, and Michael Zimmer. 2017. "Privacy Policies and Practices with Cloud-Based Services in Public Libraries: An Exploratory Case of BiblioCommons." *Journal of Intellectual Freedom and Privacy* 2 (July): 23. https://doi.org/10.5860/jifp.v2i1.6252.

Lambert, April D., Michelle Parker, and Masooda N. Bashir. 2015. "Library patron privacy in jeopardy: An analysis of the privacy policies of digital content vendors." Proceedings of the Association for Information Science and Technology. 2015. https://doi.org/10.1002/pra2.2015.145052010044.

Macrina, Alison. 2018. *Anonymity.* Neal-Schuman Publishers, Incorporated.

Magi, Trina J. 2010. "A content analysis of library vendor privacy policies: Do they meet our standards?" University Libraries Faculty and Staff Publications. https://scholarworks.uvm.edu/libfacpub/5.

Magi, Trina, M. Garnar, and Office for Intellectual Freedom. 2015. *Intellectual Freedom Manual, Ninth Edition.* Chicago: ALA.

Newman, Bobbi, and Bonnie Tijerina, eds. 2017. *Protecting Patron Privacy: A LITA Guide.* Rowman & Littlefield.

Nicolas-Rocca, Tonia San, and Richard J. Burkhard. 2019. "Information Security in Libraries: Examining the Effects of Knowledge Transfer." *Information Technology and Libraries* 38 (2): 58–71. https://doi.org/10.6017/ital.v38i2.10973.

Pedley, Paul. 2020. *A Practical Guide to Privacy in Libraries.* London: Facet Publishing.

Pekala, Shayna. 2017. "Privacy and User Experience in 21st Century Library Discovery." *Information Technology and Libraries* 36 (2): 48–58. https://doi.org/10.6017/ital.v36i2.9817.

Thomchick, Richard, and Tonia San Nicolas-Rocca. 2018. "Application Level Security in a Public Library: A Case Study." *Information Technology and Libraries* 37 (4): 107–18. https://doi.org/10.6017/ital.v37i4.10405.

Yoose, Becky. 2017. "Balancing Privacy and Strategic Planning Needs: A Case Study in De-Identification of Patron Data." Journal of Intellectual Freedom & Privacy 2 (1): 15–22. https://doi.org/10.5860/jifp.v2i1.6250.

Young, Scott W. H., Jason A. Clark, Sara Mannheimer, and Lisa Janicke Hinchliffe. 2019. "A National Forum on Web Privacy and Web Analytics: Action Handbook." https://doi.org/10.15788/20190416.15446.

Young, Scott W. H., Sara Mannheimer, Jason A. Clark, and Lisa Janicke Hinchliffe. 2019. "A Roadmap for Achieving Privacy in the Age of Analytics: A White Paper from A National Forum on Web Privacy and Web Analytics." https://doi.org/10.15788/20190416.15445.

Zimmer, Michael. 2013. "Assessing the Treatment of Patron Privacy in Library 2.0 Literature." Information Technology and Libraries. https://doi.org/10.6017/ital.v32i2.3420.

General Privacy Resources and Organizations

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

Future of Privacy Forum. https://fpf.org/.

International Association of Privacy Professionals. https://iapp.org/.

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

Tactical Tech. https://tacticaltech.org.

Pacific Library Partnership

32 W. 25th Ave., Suite 201
San Mateo, CA 94403
650-349-5538
info@plpinfo.org

Data Privacy Best Practices Training for Libraries *is supported in whole or in part by the U.S. Institute of Museum and Library Services under the provisions of the Library Services and Technology Act, administered in California by the State Librarian. The opinions expressed herein do not necessarily reflect the position or policy of the U.S. Institute of Museum and Library Services or the California State Library, and no official endorsement by the U.S. Institute of Museum and Library Services or the California State Library should be inferred. This document does not constitute legal advice, and is for informational purposes only. Please consult an attorney or other legal counsel for legal advice.*