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

Becky Yoose
Library Data Privacy Consultant, LDH Consulting Services
Pacific Library Partnership, May 2020

This project was 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.

Workshop Housekeeping - Logistics

IANAL; Consult legal staff for legal advice

Exercises and Discussions - what to expect

Toolkit tie-in

Privacy measures are only as strong as the least-knowledgeable person working with patron data

Introduce Yourself!

1. Name
2. Job title and where you work
3. What is one third party service or product you use to protect your personal privacy?

Section One:
Vendors and Libraries

Vendors in the life of the library

- Integrated Library Systems (ILS)
- Print management systems
- Reference chat applications
- Public computer management systems
- Interlibrary Loan
- Web analytic software
- Social media platforms
- Security cameras
- Card reader software
- Meeting room reservation systems
- Customer Relationship Management Systems
- Data analytic systems
- Instructors contracted to teach/lead library programs

Personally Identifiable Information [PII] and Library Data

PII 1 - Data about a patron

- Name
- Physical/email address
- Phone number
- Date of birth
- Patron record number
- Library barcode

PII 2 - Activity that can be tied back to a patron

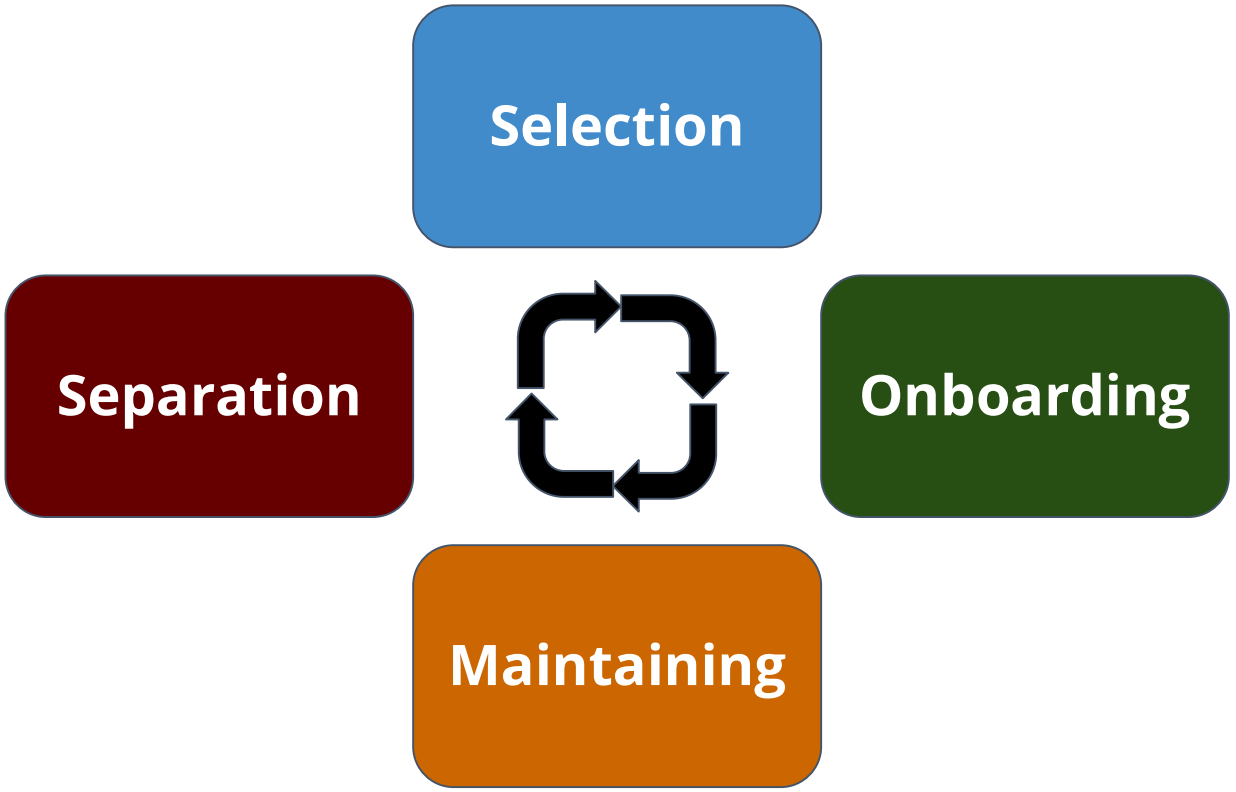
- Search & circ histories
- Computer/wifi sessions
- Reference questions
- Electronic resource access
- IP Address
- Program attendance

Library Patron Data Lifecycle

A very short list of vendor vulnerabilities

- No HTTPS support
- Unsecured server access
- Unencrypted and/or unsecured data storage
- No backups
- No record retention policy
- No database access restrictions or policy
- Improper or incomplete data scrubbing
- No strategies for data deletion when customer leaves vendor
- Collecting ALL the data
- Tracking users without consent
- Sharing patron information to third parties without consent or notification
- No public privacy policy

Vendor Relationship Lifecycle



kanopy

Good afternoon,

Over the weekend, we became aware of an issue affecting the security of our platform. We promptly resolved the issue by Monday afternoon and are taking all necessary steps to maintain the security of our systems going forward. While our investigation is ongoing, at this stage, we believe significantly less than one percent of accounts have been affected.

The only thing as important as providing our Kanopy users with rich viewing experiences is protecting the integrity and security of your data. As our community continues to grow, we will always prioritize ensuring that our platform is entirely secure, regardless of scale.

The Santa Cruz Public Library System assesses each vendor we use for multiple data privacy and protection best practices. Each vendor is required to complete a Vendor Security Assessment Questionnaire, and respond to 78 questions in 7 areas:

- *Service Overview*
- *Data Protection & Access Controls*
- *Policies & Standards*
- *Application Security*
- *Compliance*
- *Security Measures*
- *Which Data Are Collected*

Product	Vendor
Academic OneFile	Gale
Acorn TV	RBDigital/Acorn TV
America's News	NewsBank

Exercise – Reflection

Think of a time when you found or encountered an issue with a vendor that put patron privacy at risk.

1. What was the issue?
2. When and how did you find out about the issue?
3. How did the vendor respond to the issue?
4. How was the issue resolved or addressed?

(Hold on to those thoughts for later in the presentation!)

Section Two: Selection

Selection - Where to start?

RFI - Request for Information

Used to gather information about services or products

Potential uses:

- Obtain privacy policies
- Gather information about general privacy features

RFP - Request for Proposals

Used to gather bids from potential vendors

Potential uses:

- Outline privacy reqs
- Gather information about specific privacy features

Selection - RFP Functional Requirements

List specific privacy functionality and features, including:

- Regular security and privacy audits
- Patron ability to opt-in/opt-out of non-essential data collection
- Sharing of patron data to subcontractors and service providers
- Ability to adjust/set data retention settings
- Vendor privacy policy
- Vendor compliance to local, state, and other regulations
- Ability to export and delete library data at time of separation

Selection - RFP Functional Requirements

List specific information security best practices and standards, including:

- Regular security and privacy audits
- Physical and electronic access controls to library data
- Encryption of data at rest and in transit
- Secure media destruction
- Industry standards, principles or certifications
  - Example - International Organization for Standardization (ISO) certifications

Section Three: Onboarding

Onboarding - Contract Negotiations

Before you begin negotiations:

- Identify any specific issues or changes to the contract based on the findings of the RFP process
- Determine what you are willing to compromise on if pushed
- *Determine what will be the dealbreakers*

Contracts and Legal Regulations – California Gov Code § 6267

All patron use records of any library which is in whole or in part supported by public funds shall remain confidential and **shall not be disclosed by a public agency, or private actor that maintains or stores patron use records on behalf of a public agency, to any person, local agency, or state agency** except as follows:

(a) By a person acting within the scope of his or her duties within the administration of the library.

(b) By a person authorized, in writing, by the individual to whom the records pertain, to inspect the records.

(c) By order of the appropriate superior court.

Contracts and Legal Regulations – California Gov Code § 6267 (con't)

As used in this section, the term "patron use records" includes the following:

(1) Any **written or electronic record**, that is **used to identify the patron**, including, but not limited to, a patron's name, address, telephone number, or e-mail address, that a library patron provides in order to become eligible to borrow or use books and other materials.

(2) Any **written record or electronic transaction** that **identifies a patron's borrowing information or use of library information resources**, including, but not limited to, database search records, borrowing records, class records, and any other personally identifiable uses of library resources information requests, or inquiries.

Contracts and Legal Regulations – California Consumer Privacy Act of 2018 (CCPA)

Regulates the sale (and to a lesser extent collection and processing) of personal information by covered businesses

Gives California residents:

- Right to access what personal information is collected and shared with service providers and other third parties
- Right to request deletion of personal information
- Right to opt out of sale of personal information

Contracts and Legal Regulations – California Consumer Privacy Act of 2018 (CCPA)

Household information

- Part of personal information definition
- Included as part of the response to access and deletion requests
- Possible sharing of patron information to another patron if business determines they belong to the same household

13-16 year old affirmative consent

- Businesses must obtain affirmative consent from 13-16 year old users to sell personal information
- Possibilities:
  - COPPA liability
  - “Age-gating” sites and services – asking for age of users

Contract Negotiations – Incident Responses and California Civil Code Section 1798.82

Incident response (data breaches) information:

- Who will be responsible for what
- Timeline for incident response actions
- Financial liability to the vendor
- Compliance to state data breach regulations

1798.82 points of interest:

- Personal information definition
- What, when, and how of notification to breach victims as well as Attorney General (if breach affects > 500 people)
- Encryption exemption… unless the key is also compromised

Onboarding - Contract Negotiations

Other areas of negotiation:

- Privacy policy - will the vendor fall under the library's privacy policy?
- Vendor data security and privacy audits, policies, procedures
- Patron opt-in/opt-out of data collection

Onboarding - Contract Addendum and NDA

Contract Addendum

- Legal boilerplate for standard privacy and security contract language
- Can be used in both initial contract signings and renewal periods

Non Disclosure Agreement

- AKA NDAs
- Limit or prohibit sharing of patron data to:
  - Subcontractors
  - Service Providers
  - Other Third Parties

ADDENDUM
Confidentiality of Seattle Public Library Records and Data

The Seattle Public Library (SPL) collects and manages records and data which require confidentiality under one or more federal or state laws, or under recognized industry standards, including but not limited to, the following:

- Health Insurance Portability and Accountability Act of 1996
- Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009
- Children's Online Privacy Protection Act of 1998 (COPPA)
- The Privacy Act 1974 (as specified in the National Institute of Standards and Technology (NIST) SP 800-122)
- Washington State RCW 42.56.310
- Family Educational Rights and Privacy Act of 1974
- The American Library Association Library Bill of Rights
- United States Constitution, including the first and fourth amendments

Addendum (con’t)

Specifically, a provider of services to SPL will not reveal or disclose any data or records, either physical or electronic, which are designated as confidential by the Library or which pertain to SPL patrons when such data or records could be used in any manner to identify a Library patron or any references or materials that a specific Library patron accesses.

A provider of services to SPL must treat all the designated or individually identifiable SPL records as confidential and protected. Encryption of such data while in motion or at rest, and restricting access to confidential data, are typical methods of data protection. No SPL records or data shall be released by the provider to any third party without the prior written consent of the SPL.

Addendum (con’t)

In the event that the provider violates this addendum, then said provider agrees to indemnify, defend and hold harmless SPL and its employees from and against any losses, costs, expenses, liabilities (including attorney’s fees), penalties and sanctions arising out of or relating to such violation. This addendum does not limit the provider’s liability as specifically established under law.

The Parties hereto agree that this amendment modifies, changes, amends and has precedence over any contradictory language in the contract between the Parties.

Onboarding - Service Setup and Defaults

Service Settings

- Backups
- System logs
- Data retention
- Collecting patron data

Public-facing settings

Can all non-essential data sharing/collection be turned off by default?

Web trackers and patron data collection

Exercise - Importing Data

- Your library purchased a customer relationship management system primarily for the email subscription management functionality
- Vendor sends your library a data workbook asking for a wide range of patron data, including emails, full names, physical addresses, phone numbers, patron record numbers, circulation histories, program attendance, computer usage, etc.

What would you do in this instance?

Onboarding - Importing Data

How the scenario from the exercise played out in the real world:

- Vendor sends a worksheet with list of patron data to upload
  Library staff inventories all data requested by vendor
- Library staff reviews each data point to determine:
  - Operational need for data to be included in the system
  - Privacy risk level to patron and library
- Library goes back to vendor with proposed data upload
- Vendor and Library negotiate and agree on modified data upload

Onboarding – Communications

Staff

- Announcements via:
  - Email
  - Staff Intranet
  - Meetings
- Vendor privacy notice list
- Update privacy policies if necessary

Patrons

- Press releases or news announcements
- Vendor privacy notice list on public site
- Update privacy notice if necessary

Log In

Adjust your privacy settings by visiting 'My Settings & Privacy'. By default, Lists and Shelves are visible to other users. **Your library borrowing activity - items you browse, check out, place on hold, return, etc. - remains confidential in accordance with the Library's policy.**

Username or Barcode:

PIN:

Forgot your PIN?

New to the Catalog? Create your username to get started!

Enter your library card barcode or confirmation number, and your 4-digit

This is a Connected Library

If you already have an online account registered at **King County**, you can link your online accounts

Section Four: Maintenance

Maintaining

- Regularly schedule security/privacy audits with vendors
- Privacy and security as a standing meeting topics
- Review any changes in local, state, national, or other regulations and how those changes will affect data privacy practices
  - Examples:
    - General Data Protection Regulation (GDPR)
    - California Consumer Privacy Act (CCPA)

Maintaining – Vendor Changes in Contract or Functionality

Renegotiate Contract

- Renegotiate contract with vendor, including adding an addendum
- Lots of back and forth, lots of legal counsel meetings, may end up with compromise

OR

Not Renew Contract

- Additional selection, onboarding, etc. for new vendor
- New vendor might be more willing to take into account library concerns

FOR IMMEDIATE RELEASE

July 22, 2019

Alex Vassar
Communications Manager
(916) 653-3883
press@library.ca.gov

California State Library Recommends Libraries Not Provide LinkedIn Learning Due to Privacy Concerns

Sacramento, Calif. – The California State Library recommends libraries no longer use or provide LinkedIn Learning to their patrons until the company changes its use policy to protect the privacy of library users.

The statement by State Librarian Greg Lucas:

LIBRARIES

LinkedIn Pauses Changes to Lynda.com After Libraries Raise Privacy Concerns

By Jeffrey R. Young Nov 27, 2019

Grenar / Shutterstock

EMAIL

LinkedIn has temporarily delayed planned changes to Lynda.com, a popular education-video library the company bought in 2015 for $1.5 billion, after libraries around the country raised privacy concerns.

Exercise - To Talk or To Leave

Your reference chat application vendor included an item in their revised contract that allows them to use data collected by the application to build a cloud chatbot service that can automatically answer questions as they come into the chat queue. Chat data:

- Does not include name, email, or other data about a person
- Includes chat questions and answers

1. What are the potential privacy risks with this change?
2. What possible negotiation strategies would you use during the renewal process?
3. Would this be a dealbreaker? Why or why not?

Section Five: Separation

Separation - Ending the Relationship

- Plan for the separation before it happens
  - Contact addendum
  - RFP information
  - Privacy audits
- Export and deletion rights for:
  - The library
  - The patron
- What happens to your data when you leave?
  - Deletion or ...?

Exercise – Do-over

Knowing what you know now from the presentation, what strategies, tools, or practices might have helped in resolving the vendor privacy issue from the reflection exercise?

Section Six:
Other Types of Library-Third Party Relationships

Special Cases - School Data Sharing

Receiving student data for special programs and services offered by the library

- Common example - school student data used to create public library cards for students to access electronic resources
- Contract negotiations
  - Lay out handling policies/procedures for student data with Family Educational Rights and Privacy Act (FERPA) guidelines in mind
- Maintenance
  - Separate student data from any data exports to vendors or other third parties

Special Cases - Open Data Initiatives

City or organizational policy to publish data to the public

Common example - Civic open data programs (San Francisco, Seattle, Chapel Hill)

Work with initiative staff in determining security and privacy policies and procedures surrounding data selection and publication

Some open data initiatives are “open by default”, others “open by preference”

Privacy impact assessment for potential data set publication

Section Seven:
Wrap up

Next Steps, or Places to Start

- Contract addendum drafting
- Review contracts during renewal periods
- Work with staff responsible for RFI/RFP and purchasing for your library in incorporating functional requirements and contract addendums
- Data inventories of major vendor services
- Set up schedule for vendor security and privacy audits

What is one thing from this workshop that you can put into practice or discussion at your library when you return?

But wait – there’s more!

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

May 19th and May 20th

Thank you

:-)

LDH Consulting Services

Becky Yoose
Library Data Privacy Consultant
LDH Consulting Services

Email:
becky@ldhconsultingservices.com