Privacy-Centered Library Vendor Management

Becky Yoose
Library Data Privacy Consultant, LDH Consulting Services

Colorado State Library, 3/3/2020

Housekeeping

Resource list available in the handout

IANAL; Consult legal staff for legal advice

Exercises and Discussions - what to expect

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

Vendors in the life of the library

- Integrated Library Systems (ILS)
- Print management systems
- Reference chat apps
- Public computer management systems
- Web analytic software
- Security cameras
- Card reader software
- Customer Relationship Management Systems
- Data analytic systems
- Instructors contracted to teach/lead library programs

Personally Identifiable Information [PII] and Library Data

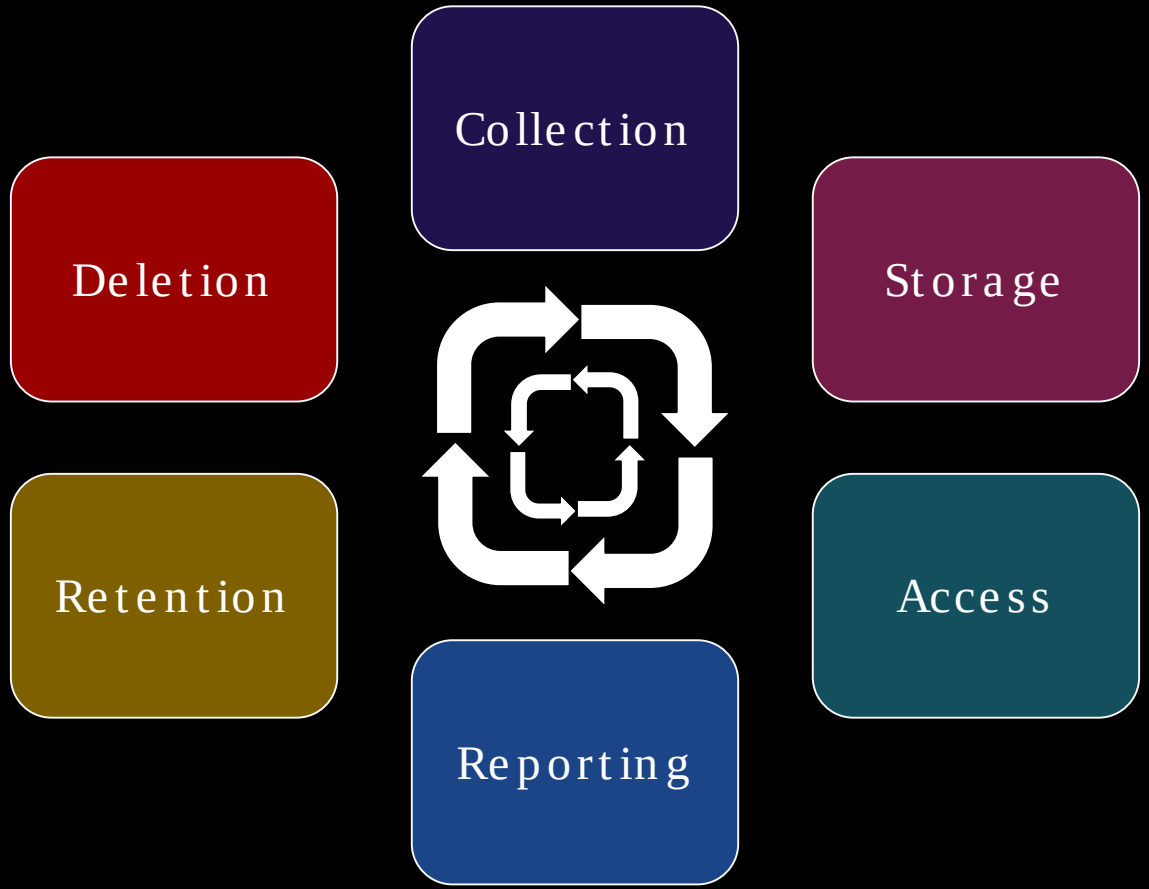
PII 1 - Data about a patron

- 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 & circulation 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

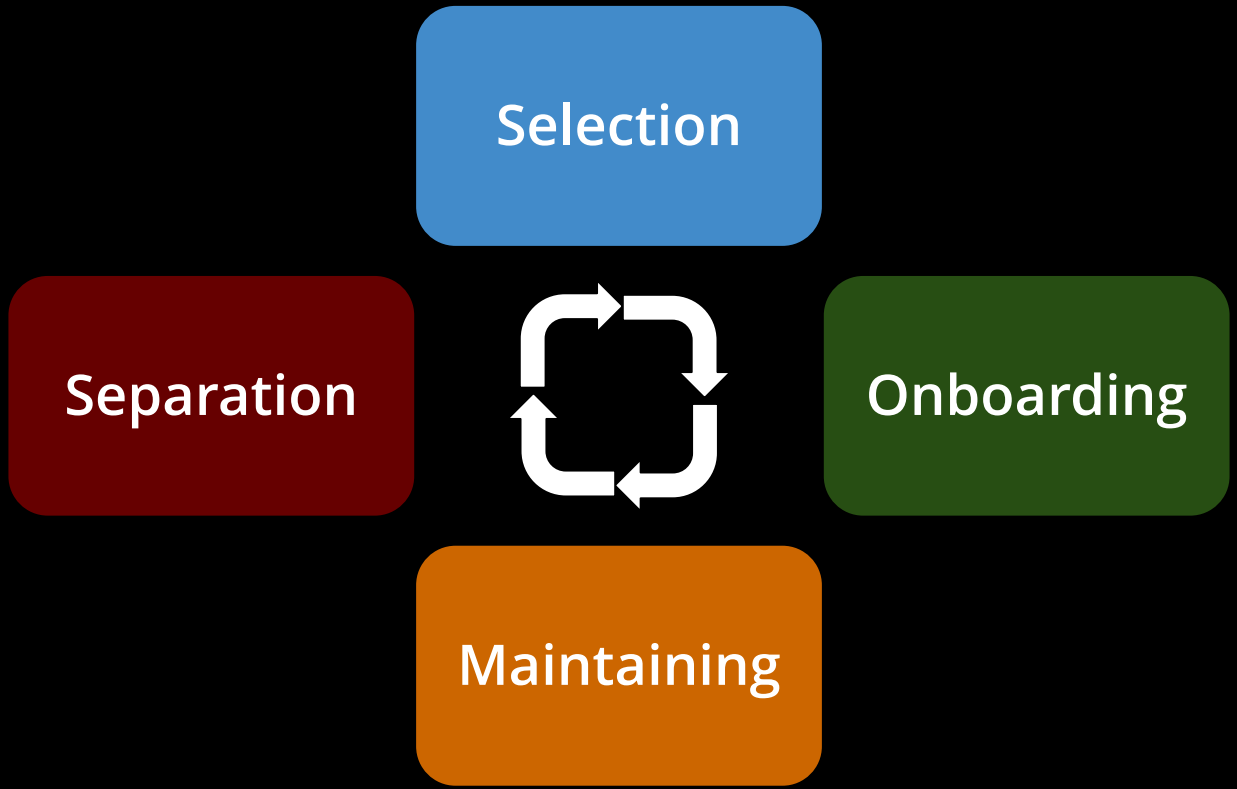
Exercise – Reflection

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!)

Vendor Relationship Lifecycle



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:

- 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

Onboarding - Contract Negotiations

Before you begin negotiations:

- Identify specific issues from vendor’s RFP response
- Work with legal counsel to identify changes to the contract
- Determine what you are willing to compromise on if pushed
- *Determine what will be the dealbreakers*

Onboarding - Contract Negotiations

Areas of negotiation:

- Privacy policy – the library's or the vendor's?
- Incident response (data breaches, leaks, etc.)
  - Outline responsibilities for both sides
  - Timeline for incident response actions
  - Financial liability to the vendor
  - *Compliance to state data breach regulations*
- Vendor data security and privacy audits, policies, procedures
- Opt-in/opt-out of patron data collection

Onboarding - Contract Addendums and NDAs

Contract Addendums

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

Non Disclosure Agreements

- AKA NDAs
- Limit or prohibit sharing of library patron data under most circumstances 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
- Data collection

Public-facing settings

- Can all non-essential data sharing/collection be turned off by default?
- Web trackers and patron data collection

Onboarding Example - Importing Data

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

Maintaining

- Regularly scheduled vendor security/privacy audits
- Privacy as standing meeting topic
- Review any changes in local, state, national, or other data privacy regulations
    - 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

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?

Separation - Ending the Relationship

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?

Special Cases - School Data Sharing

- 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 (NYC, 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

Next Steps, or Places to Start

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

Thank you
:-)

Becky Yoose
Library Data Privacy Consultant
LDH Consulting Services

Email: becky@ldhconsultingservices.com