

# Beyond Data Privacy Training

Becky Yoose  
Library Data Privacy Consultant, LDH Consulting Services  
Data Privacy Best Practices Training for Libraries  
April 2021  
Week 3



---

---

---

---

---

---

---

---

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.



---

---

---

---

---

---

---

---

## Today's Schedule

1:00 – 1:20 Welcome and course housekeeping  
1:20 – 1:45 Training  
1:45 – 1:50 Break  
1:50 – 2:25 Training  
2:25 – 2:30 Wrap up

---

---

---

---

---

---

---

---

## Last Week Recap



---

---

---

---

---

---

---

---

## Series Housekeeping – Guidelines

- When you disagree, challenge or criticize the idea, not the person.
- Speak from your own perspective.
- Be mindful of the time.
- One speaker at a time.
- What is said in this space, stays in this space unless you have permission.

---

---

---

---

---

---

---

---

## 0. Housekeeping – The Kitchen Sink

---

---

---

---

---

---

---

---

## The Sink

- Privacy Risk Management
- Vendor Management
- Patrons and Data Privacy



---

---

---

---

---

---

---

---

Tie everything together



---

---

---

---

---

---

---

---

1. Privacy Risk Management

---

---

---

---

---

---

---

---

## Risk = Threat x Vulnerability x Cost

- **Threat**
  - Potential scenario that can cause damage or loss to an organizational asset
- **Vulnerability**
  - Weakness in any system or structure that a threat can use to cause harm to the organization
- **Cost**
  - Potential impact, be it monetary, reputational, legal, operational, etc. on organizations and people targeted by threat

(Likelihood and Severity are also factors in calculating risk)

---

---

---

---

---

---

---

---

## Discussion – (Risk = Threat x Vulnerability x Cost) + Libraries

---

---

---

---

---

---

---

---

## Risk Assessments

### **What do we have?**

- Data Inventories
- Recording where data lives in the library and beyond (in the case of external departments and vendors)
  - Tracking data through the data lifecycle (collection, storage, etc.) as well as how the data is used, who is using/disclosing data, and why

### **We can, but should we?**

- Privacy Impact Assessments (PIA)
- Evaluates new and changing processes or systems for compliance to legal regulations and policies
  - Assesses privacy risks presented by processes or systems
  - Identifies and examines possible ways to mitigate risks in processes or systems

---

---

---

---

---

---

---

---

## Addressing Risks - Strategies

### **Accept**

- Risk to org or person is low
- Resource restrictions

### **Mitigate**

- Privacy controls can be implemented in the process or product to limit risk

### **Transfer**

- Risk can be better managed by another entity, product, or process

### **Eliminate**

- Changes to product or process to avoid identified risk

---

---

---

---

---

---

---

---

Poll – Accept,  
Transfer, Mitigate,  
or Eliminate?

---

---

---

---

---

---

---

---

1.5 Library Privacy Policy and  
Procedures

---

---

---

---

---

---

---

---

## Risk Reduction – Policies and Procedures

### **Policies**

- The “what” and “why”
- A library must have a Patron Privacy & Confidentiality Policy
- Policies are shaped by legal regulations, professional ethics/standards, and best practices
  - California laws
  - Local laws (e.g. retention schedules)
  - Federal laws (when applicable)

### **Procedures**

- The “how, when, where, and who” of policy implementation
- Who will use the procedure and how the documentation will be used?
- Procedure matching policy, policy matching procedure
- Guidelines as procedures

---

---

---

---

---

---

---

---

## Risk Reduction – Policies and Procedures

- Data collection, use, storage, and retention based on data classifications
  - High/Medium/Low Risk
  - Confidential/Sensitive/Private/Public Information
  - Personally Identifiable Information (PII)/Non-personal Information
- Regularly scheduled data inventories
- Identifying “trigger” events that would initiate a data inventory or PIA process
  - Selection of a new application, new work process, changes in procedure/policy, changes in vendor product/services

---

---

---

---

---

---

---

---

## 2. Vendors

---

---

---

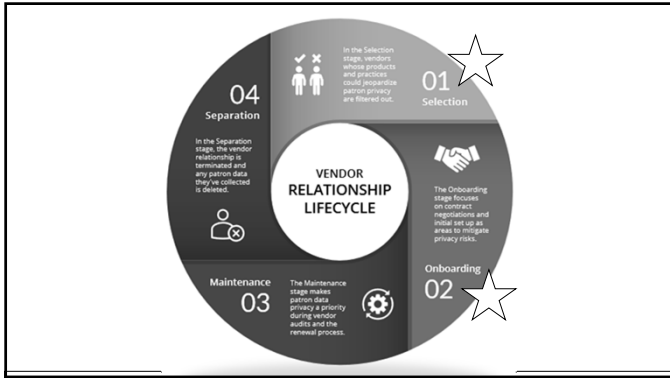
---

---

---

---

---




---

---

---

---

---

---

---

---

### Selection

<p><b>RFP - Request for Proposals</b></p> <ul style="list-style-type: none"> <li>Used to gather bids from potential vendors</li> <li>Potential uses: <ul style="list-style-type: none"> <li>Outline privacy requirements</li> <li>Gather information about specific privacy features</li> <li>Gather information about data practices, including collection, processing, and disclosure</li> </ul> </li> </ul>	<p><b>Privacy and Security Functional Requirements - Examples</b></p> <ul style="list-style-type: none"> <li>Ability to opt-in/opt-out of non-essential data collection and/or disclosure</li> <li>Meets/exceeds industry security standards</li> <li>Compliance to legal regulations</li> <li>Privacy policy</li> </ul>
--	--

---

---

---

---

---

---

---

---

### Contract Red Flags

<ul style="list-style-type: none"> <li>"Reasonable" and other vague terms</li> <li>Lack of definitions for terms</li> <li>Indemnity/liability clauses</li> <li>Termination details - data exit</li> <li>Lack of information about responses to law enforcement or government data requests</li> <li>Legal jurisdiction!</li> </ul>	<ul style="list-style-type: none"> <li>Lack of transparency</li> <li>Data ownership</li> <li>Data reselling or disclosure to other third parties</li> <li>Monitoring patron use (web analytics)</li> <li>Using "Aggregated", "Anonymized", "De-identified" without defining methods</li> </ul>
--	--

---

---

---

---

---

---

---

---

## Negotiations (Or How to Be A Good Advocate for Patron Privacy)

- Contract Addendums (vetted by legal staff) Are Your Friend
- Patron data rights (under CCPA/CPRA, GDPR when applicable) and opt-in/opt-out rights
- Negotiate privacy protections around collection, use, disclosure, retention, and deletion
- **You don't have to sign contracts that put patron privacy at risk.**
  - It helps to have some backup from other libraries and organizations.
    - This strategy works if enough libraries advocate for privacy practices (e.g. LinkedIn Learning).
  - Is the compromise worth the risk to the patrons who will experience the greatest amount of harm if something goes wrong?

---

---

---

---

---

---

---

---

Discussion – Should I stay or should I go?

---

---

---

---

---

---

---

---

3. Patrons and Data Privacy

---

---

---

---

---

---

---

---



## Library Use and Privacy – Data Exhaust

- Public computers & WiFi
  - Reservation systems
    - Logs
    - Data collection/retention in reservation process
  - Computer Images
    - Installed tools and apps
    - System/application logs
  - Network
    - IP addresses
    - Traffic logs
    - Accounts accessing network (if requiring sign-in for WiFi)
- Meetings rooms
  - Reservation systems
    - Data collection/retention in reservation process
- Printers, copiers, scanners, fax machines
  - Memory storage
  - “Abandoned” printing jobs
- Surveillance
  - Security camera footage
  - Incident reports
  - Event recording (online and physical events)

---

---

---

---

---

---

---

---

## Library Use and Privacy – Data Exhaust, Sources, and Use Expectations

- Library Websites and...
  - Web analytics
  - Social media
- Vendor resources and...
  - Authentication
  - Proxy URLs
  - User accounts
  - Web analytics
  - Other data exhaust
- **Patron data sources and uses**
  - What data is given to the library by the patron vs data collection without explicit awareness
  - Primary vs secondary uses of data
    - What does the patron expect vs how the library actually uses data
  - Example - Marketing and data analytics and external data sets containing data about patrons

---

---

---

---

---

---

---

---

## Library Vendors and Patrons

- Vendors collecting data from the library vs vendors collecting data from patrons
- Vendor communications about privacy to patrons
  - Deceptive patterns around privacy settings/information
- Library communications about vendor privacy practices to patrons
  - Privacy policy, vendor privacy policy page, website alerts, etc.



---

---

---

---

---

---

---

---

## Patron Communications

- Privacy notice
  - Be accessible in both online and in physical formats
  - Explain privacy policies and patron privacy/confidentiality rights in simple, concise language to a general audience
  - Published in the major languages of the service population
  - Inform the reader of any policy changes
- Press releases, blog posts, newsletter updates
- Website alerts and popups are limited in their effectiveness – use judiciously
- Dialogue with community partners and organizations

---

---

---

---

---

---

---

---

## Patron Privacy Programming and Services

- Digital literacy
- Information security and privacy
- Device security



---

---

---

---

---

---

---

---

## Patron Privacy as a Service (PPaaS)

### **San Jose Public Library's Virtual Privacy Lab**

- Customized privacy toolkits based on patron's needs and risks
- Individual toolkit modules about specific privacy topics:
  - Social media
  - Security
  - Information footprint
  - Anonymity & tracking
- In-depth modules for intermediate/advanced learning

### **Cornell University Libraries' Privacy Services**

- Digital privacy literacy
  - Individual consultations
  - In-class or customized workshops
  - Open drop-in workshops
- Privacy risk consultations
  - Digital communication with human subjects whose anonymity must be protected
  - Crossing the U.S. border
  - Personal identities with an increased risk of doxing, harassment, or surveillance

---

---

---

---

---

---

---

---

## Questions and Open Discussion

---

---

---

---

---

---

---

## Wrap Up

---

---

---

---

---

---

---

## Next Week

### **Week Four - Building and Fostering a Culture of Privacy**

- April 28<sup>th</sup>, 1 pm – 2:30 pm
- Register at <https://www.plpinfo.org/event/building-and-fostering-a-culture-of-privacy-2/>

### **Week Three Activities/Reading**

- Year One Toolkit, Sections 2 (pg. 14-15), 3-5
- Exercises on Basecamp

---

---



---

---

---

---

---

<p>Thank you</p> <p>: -)</p> 	<p>Becky Yoose Library Data Privacy Consultant LDH Consulting Services</p> <p>Email: becky@ldhconsultingservices.com</p>  <p><small>This work is licensed under a <a href="https://creativecommons.org/licenses/by-sa/4.0/">Creative Commons Attribution-ShareAlike 4.0 International License</a>.</small></p>
--	---

---

---

---

---

---

---

---

---

<p>Resources and Further Reading</p> <p>Additional bibliographies and resources can be found in the Toolkit and training resources at the <a href="https://www.plpinfo.org/dataprivacytoolkit/">https://www.plpinfo.org/dataprivacytoolkit/</a>.</p>
--

---

---

---

---

---

---

---

---