Beyond Data Privacy Training

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

Pacific Library Partnership

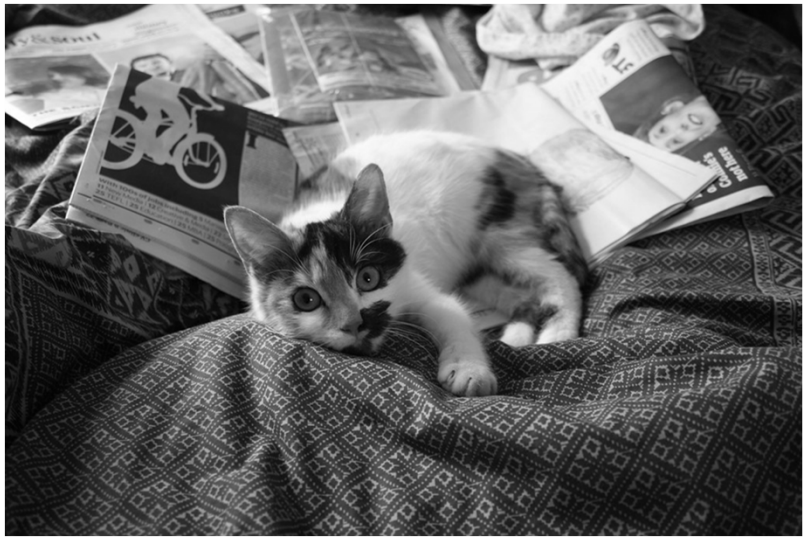
Welcome back to the third week of the series! Today's webinar is going to be a whirlwind tour of three key areas in protecting patron privacy – risk assessment, vendor selection and contracts, and patron programming and communications.

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.

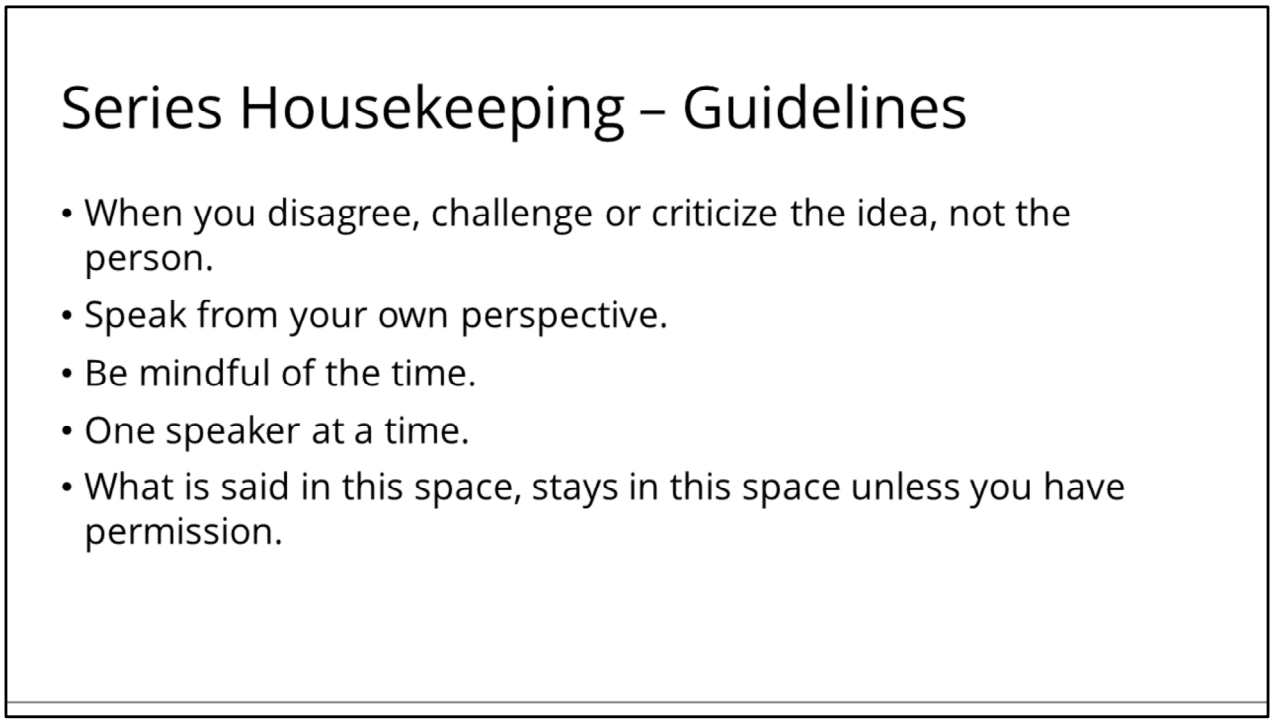
This is a quick FYI that this workshop is part of a project supported by the Library Services and Technology Act, so thank you to the grant authority for providing resources for this project. You can find this statement in your handouts as well.

This privacy train the trainer webinar series runs on Wednesdays in April from 1 to 2:30. Each week we'll try to keep close to the schedule posted in the slide. There will be some time for Q&A at the end of the session, so if any questions pop up during the presentation, you can enter them in the chat box so we can answer them then.

Last Week Recap



[Image description: a white, orange, and black calico kitten lays on a pile of newspapers on a red blanket.]
[Image source: https://www.flickr.com/photos/andres-y-linda/445989772/ (CC BY ND 2.0)]



We will be doing a good amount of discussion in this series and to help create an inclusive learning environment, I ask that everyone use this slide to help guide their interactions

- When you disagree, challenge or criticize the idea, not the person.
- Speak from your own perspective. "I" statements are useful ways for keeping from generalizing about what others think or feel.
- We'll have some time for discussion, but it's always helpful to be mindful of the time while you are speaking.
- Online conversations can get busy quickly, so speaking one at a time can help mitigate confusion and overlapping conversations
- This session will not be recorded, so you have some leeway as to what can be discussed off the record. Only attribute what is said in this space to an individual if they give you permission.

0. Housekeeping – The Kitchen Sink

As I mentioned, this week will not be like the deep dive we had about privacy training last week. Why is that?

The Sink

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

We can be advocates for privacy training but we also need privacy advocates beyond training. As you start talking to your colleagues, you might find some people concerned about specific privacy issues who could then become privacy advocates for those issues. Some of the shared concerns and interests from people who answered the PLP survey late last year included risk management, vendor management, and all things patron services and programming.

This session might come off as a kitchen sink approach…

[Image description: A black and white cat laying down in a stainless steel kitchen sink.]
[Image source: https://www.flickr.com/photos/helloturkeytoe/5486567863/ (CC BY 2.0)]

Tie everything together

There are a couple of ways you can tie everything together! You can tie these topics back to the patron data lifecycle. We'll be also tying everything together when we talk next week about creating a culture of privacy at the library. By having these areas on your privacy radar, you can start thinking of ways to approach privacy beyond offering privacy trainings at the library.

[Image description: A long haired black and white cat wearing a small purple fedora hat and a red and black plaid bow tie.]
[Image source: https://en.wikipedia.org/wiki/File:TheOreoCat.jpeg (CC BY SA 4.0)]

1. Privacy Risk Management

With that in mind, the first section, privacy risk management, is where we figure out what is a risk, how do we assess that risk, and what to do about it.

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)

For those not used to thinking about risk assessment, figuring out what is a risk can be a challenge. There is an equation that you can use to identify risk. Risk is the potential cost resulting from a threat taking advantage of a vulnerability.

A Threat is a potential scenario that can cause damage or loss to an organizational asset. You might have heard the term threat actor, which refers to a specific someone or something that could do harm to the organization. Note well that you do not have to demonstrate malicious intent to be a threat actor. Unintentional actors are still a threat due to them exploiting a vulnerability in the organization.

Vulnerabilities are weakness in any system or structure that a threat exploits to cause harm. People focus on technical vulnerabilities; however, the non-technical vulnerabilities, aka your fellow humans and organizational structures, are as capable to be exploited by threats as your technical vulnerabilities.

Cost is the potential impact, be it financial, reputational, legal, other types of impact on both the organization and the people targeted by the threat. Your library can suffer reputational damage if there is a data breach, and your patrons might suffer financial harms if their identity is stolen using the data that was breached, for example.

You also need to take severity (the level of impact if the risk is realized) and likelihood (the chances that the risk will actually be realized) into consideration.

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

Following the equation we just covered, what would be one or two data privacy risks at your library?

Take one minute to silently jot down the risk, breaking it down to threat, vulnerability, and potential cost.

Follow-up - How does your library approach identifying privacy risks?

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

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

Data inventories are your starting point in any process where you need to figure out what types of privacy risk your library has in their dealings with patron data. Data inventories record what data is being collected, where it is being stored, how data is being used and shared with others, as well as data ownership and governance. Libraries can use data inventories to map the data lifecycle in one particular 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.

Data inventories are also a part of the Privacy Impact Assessment, or PIA, but the PIA is different from a data inventory in several ways. 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. 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

This week's readings as well as the training materials from 2020 contain more information about each process, as well as templates for data inventories and PIAs.

Addressing Risks - Strategies

Accept

- Risk to org or person is low
- Resource restrictions

Transfer

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

Mitigate

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

Eliminate

- Changes to product or process to avoid identified risk

Once you have identified the risks, it's time to decide how your library is going to address them. Documentation is key throughout the risk assessment process, but it is particularly important in this part of the process to ensure that your decisions are communicated to the organization.

There are four categories of responses to risk:

The first is to accept the risk. Sometimes the likelihood or severity of a risk is very small, or the cost of the risk being realized would cost less than trying to remedy the risk. Sometimes you don't have resources to address all risks. If you choose this response, document your rationale well, as well as any potential consequences of when the risk is realized.

The second is the transfer the risk. This is where you find a risk that might be better managed outside of the current process or system and in places that are better equipped in handling the risk. Another transfer option is to transfer the risk to another person or department that have the resources and knowledge to handle the risk. Don't be afraid to ask for help from other departments in your organization! You're not changing the process, just shifting parts of the process to others in this response.

If you decide that you need to address the risk instead of accepting or transferring the risk to someone else, you have two options. The first option is to mitigate the risk where you build in privacy controls into the system or process. If we were evaluating the risk of unauthorized access to patron data in an application, for example, one way to mitigate that risk is to use the user roles or permissions function in the application to restrict access to patron data to only those who absolutely need it for their daily duties.

The second option is to eliminate the risk. The difference between mitigate and eliminate is that while mitigation focuses on inserting privacy controls in the existing process, elimination goes a step further and requires changes in the product or process in order to get rid of the risk. This could include changes in data collection, storage, and processing. One common example of changing a process deals with driver's license numbers and address verification. Many libraries collected drivers license numbers in the patron record as part of the address verification process. This creates a risk of identity theft if the data is leaked or breached. We can eliminate the risk by changing the address verification process to not record drivers license numbers in the patron record and instead indicate in the record that the address was verified by a staff member. Another way you can eliminate risk is if the product you're evaluating just doesn't have the functionality to put privacy controls in place. You can decide then to eliminate the risk by not purchasing that product.

Poll – Accept, Transfer, Mitigate, or Eliminate?

Poll question – which is the most common way that your library addresses privacy risks?

Poll options:
Accept
Transfer
Mitigate
Eliminate
Other/none (reply in chat)

Follow-up discussion – what does your library do in terms of deciding how to address risk?

1.5 Library Privacy Policy and Procedures

We’re going to take a small detour to talk about how to create policies and procedures that reduce risk instead of increasing it. This topic is covered in depth in the Operationalizing Library Privacy: Policies, Procedures, and Practice training from 2020, but we’ll do a quick overview today.

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

Policy is your “what” and “why” document. Policy provides the high-level framework for your organization’s operations. It is also the place where you can ensure that your organization is in compliance with legal regulations, professional standards, and other policies in your organization. A library must, at minimum, have a Library Privacy and Confidentiality of Library Patron Data Policy, but this policy should also be accompanied by privacy-adjacent policies, such as telework and incident response.

Procedure is the “how, when, where, and who” document. Procedure allows you to address specific concerns and considerations of implementing policy in various areas, such as a department or project group. Procedures need to reflect the privacy policies of the library. They also should reflect how staff are going to use them. 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 at the moment. What will help them is a document that is easy to follow – such as a numbered list, bullet points, short sections, or even a visual diagram – so staff can quickly process procedure information on short notice.

Guidelines can exist alongside procedures. While guidelines are less prescriptive than procedures, they help library workers by providing parameters in which to operate in, including tie-backs to policy, and other considerations, allowing staff to use their best judgement

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

Your library might already have data classification policies, either from your parent organization or local government. You can structure policies and procedures around these classifications by specifying any restrictions or special instructions based on data classification. A common example is high/medium/low risk classification:

- High risk – personal data that is most likely to cause harm to both patrons and the library if breached or leaked
- Medium risk – personal data that can cause harm if leaked or breached when combined with at least one other data point
- Low risk – non-personally identifying data

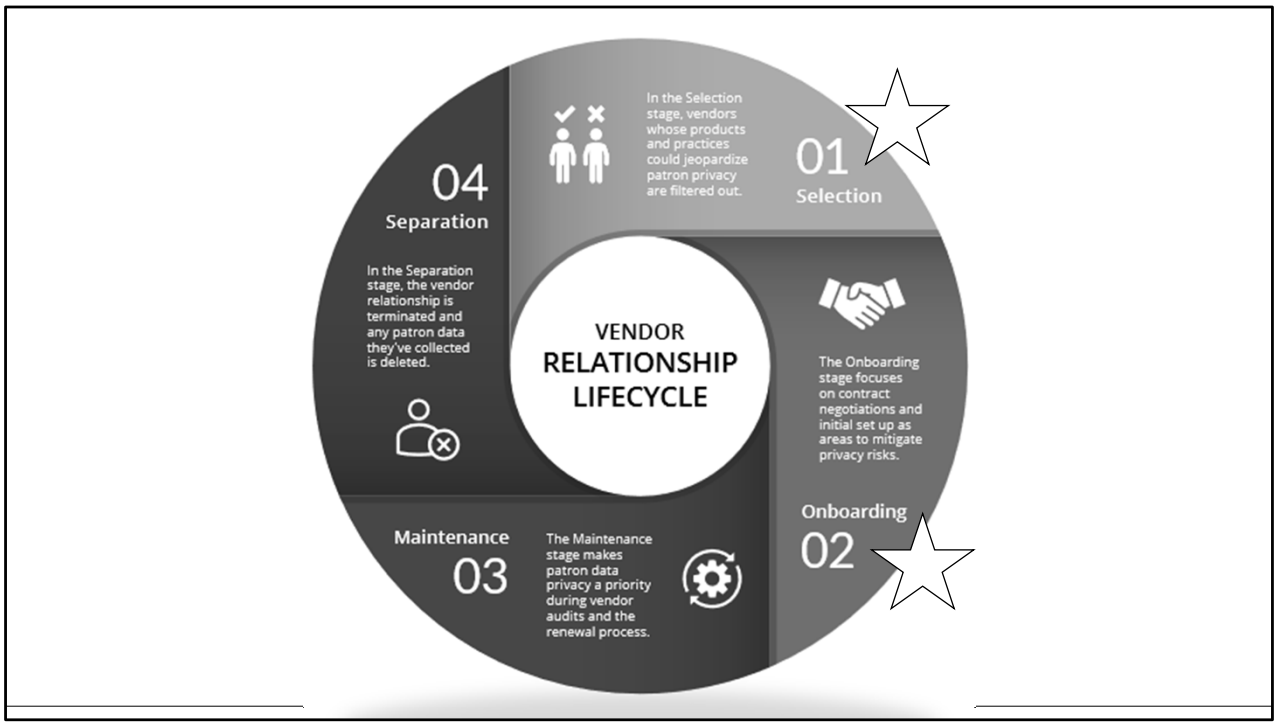
Other classifications shown in the slide follow similar patterns.

Having a regularly scheduled data inventory can help catch any possible risks that might have fallen through the cracks. However, there are times where an assessment needs to happen sooner than the annually scheduled inventory. Specify in your policies and procedures when there should be a data inventory, or when there needs to be a threshold analysis done to determine if a PIA needs to be conducted. This could include major

changes in policy or procedure, the acquisition of a new product, or a new process.

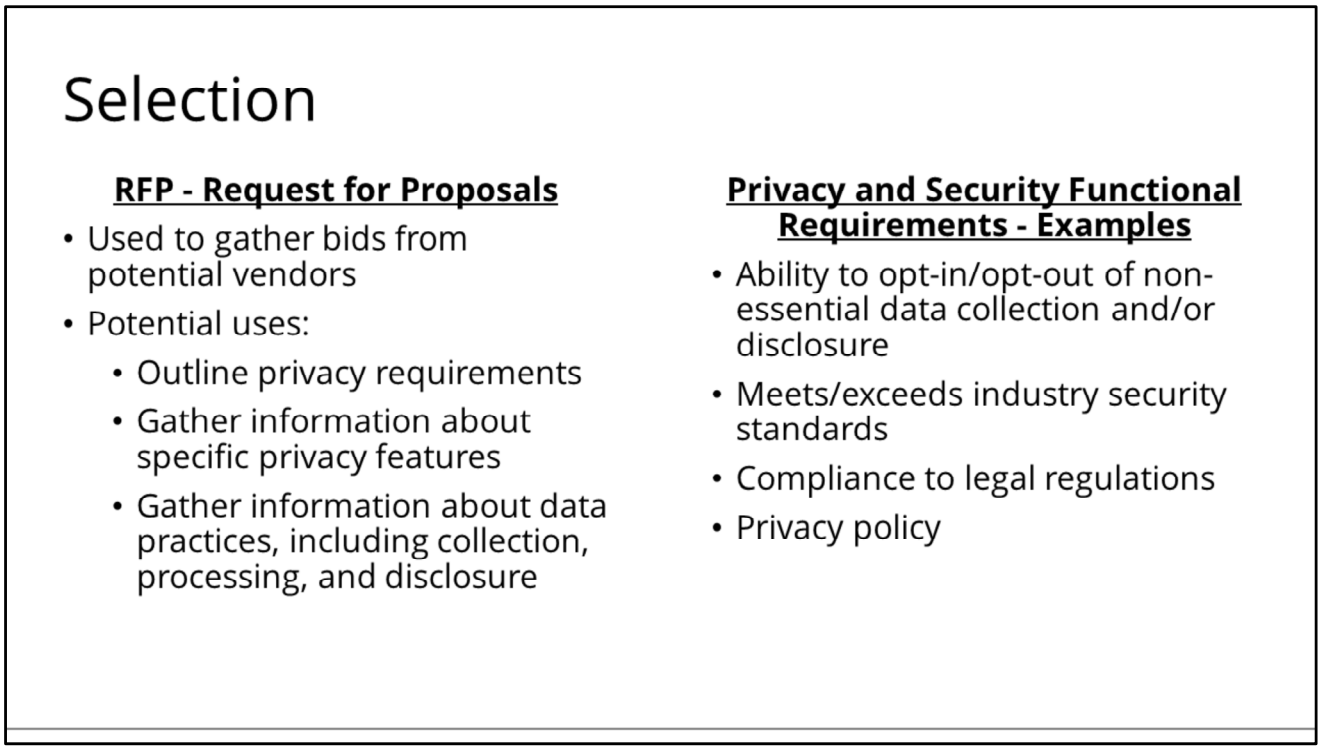
2. Vendors

Speaking of acquisitions of new products, it’s time to talk vendors and privacy. Libraries rely on vendors to handle core library services. Vendor systems collect and process patron data; however, unlike locally owned library systems and processes, libraries have limited control over the data lifecycle with any vendor service or application.



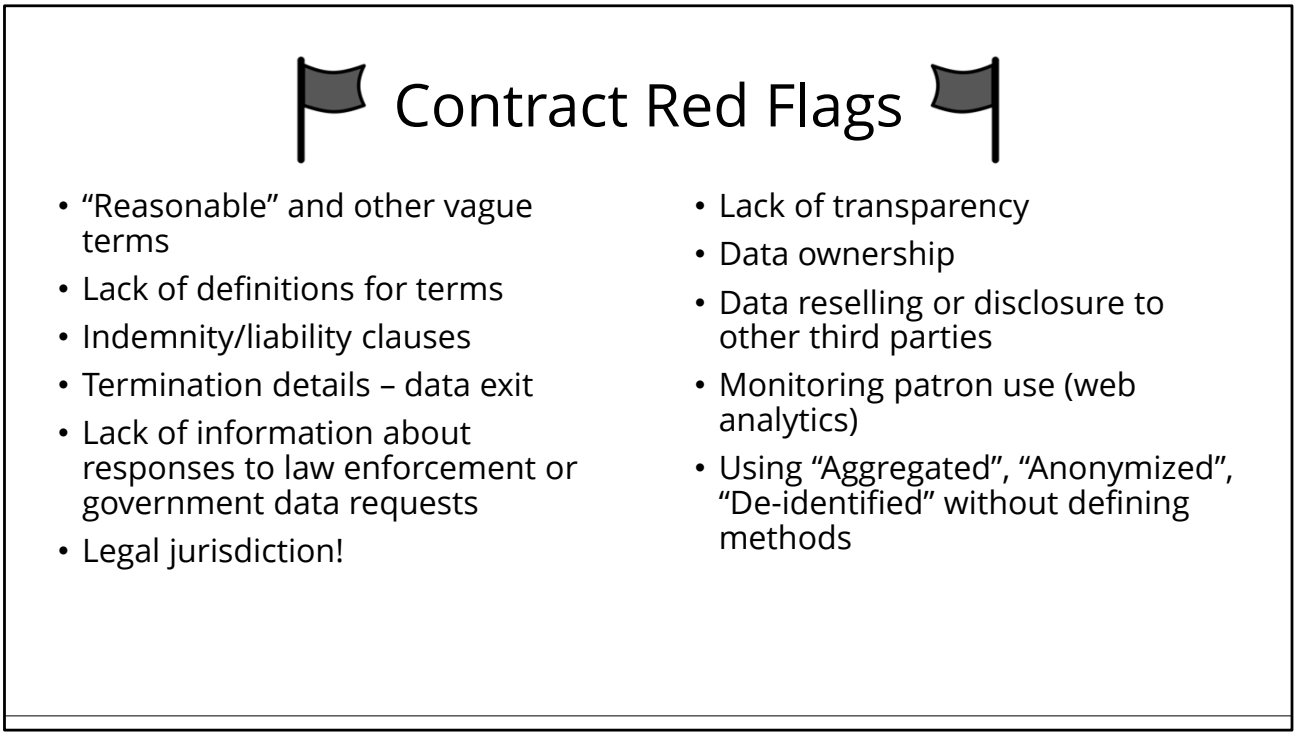
The vendor relationship cycle can help your library identify and mitigate vendor privacy risks. The cycle starts with the selection process, then working with the vendor, and then the eventual end of the business relationship. We covered this cycle in depth in the Library Privacy and Vendor Management training series in 2020. Today we are going to focus on the first two stages that have the greatest impact on privacy at your library: Selection and the contracting portion of the Onboarding stage.

[Image description: A circle flowchart illustrating the Vendor Relationship Lifecycle, starting with Selection, Onboarding, Maintenance, and Separation. Selection and Onboarding are marked with black stars.]
[Image source: Data Privacy Best Practices Toolkit for Libraries]



The library has the most control over in the vendor relationship lifecycle in the selection stage. Depending on your library, you might have a process that includes a Request for Proposal or 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.

RFP templates typically contain boilerplate language around budgetary, service, and technical requirements. You can also take this approach to create a template of privacy and security functional requirements. Before you reach a final decision to buy, you can use functional requirement questions or statements to identify vendors that allow for certain patron data rights, such as the ability to control non-essential data collection and disclosure. You can also find out if vendors meet or exceed industry standards on data security, like ISO information security standards, as well as if they comply with certain legal regulations. Asking for a privacy policy from the vendor can save you some trouble down the road in the negotiation process when determining which privacy policy the contract should follow.



The onboarding stage is fraught with hidden privacy risks. This is partially due to one key document – the contract. What *exactly* should you look out for when reading a vendor contract for the first time?

On the slide are just a few of the major red flags to look out for when reading vendor contracts. Contracts might have vague language – a common example of this is when the vendor states that they take "reasonable measures to protect data" but then don't describe how they protect the data. Sometimes they don't even define important terms – going back to that example, what does "data" mean? What actual data does it cover?

One common flag to look out for are indemnity or liability clauses which hold the vendor harmless if something goes wrong, particularly if that something going wrong is on their end.

Other flags include lack of general transparency, lack of what happens when the business relationship ends, and the vendor claiming ownership over the data you and your patrons give them. Speaking of data, some vendors write into the contract that they are allowed to disclose or resell data to other third parties for marketing or for other non-essential purposes. Other contracts have clauses that allow vendors to monitor patron use of the service, such as web analytics, for the vendor's own purposes.

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?

The contract negotiation process can be tedious, but there are a few ways to get through the process.

Contract addendums can ensure a consistent approach to vendor negotiations. They are your boilerplate for privacy and security language and requirements. Once vetted by legal counsel, addendums can help negotiate risk minimization in the data lifecycle, stating any requirements or restrictions over collection, primary use, retention, and disclosure of data to third parties.

One particular thing to include in your negotiations are patron data rights, including the right to access and delete data, and the right to control non-essential data collection and disclosure. The vendors who must comply with CCPA and CPRA should already have some process in place for patrons to exercise their right.

Ultimately, you have to weigh the privacy risk against the benefit of buying the product. You don't have to sign contracts that put patron privacy at risk. This might be tricky if the vendor is one of the few to offer a product or service; however, as demonstrated by libraries not renewing LinkedIn Learning en mass in 2019 and early 2020, vendors can be persuaded to change risky privacy practices if there is enough pressure from customers.

Discussion – Should I stay or should I go?

It’s most likely that you’ve been in contract negotiations or renewal processes where there was a major privacy concern that made you think twice about signing the contract or renewal.

If you had a situation like that, what was the issue, and how did you address the issue in the contract negotiation or renewal process?

3. Patrons and Data Privacy

Our last section gets into how patron use of the library can put them at risk and how libraries can address that risk, including communications and programming and services.

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)

Patrons create data through their use of the physical library. This includes public computers, the library network, printers, and copiers. Some of this data clearly identifies a patron – the computer reservation system log might collect username or barcode number. But this space contains some legal fuzziness when it comes to if the data is considered personally identifiable information.

California Government Code Section 6267 requires libraries and entities acting on behalf of a library to keep patron data in the library confidential. This data, called 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. However, the definition of patron use data is broad and has a lot of room for interpretation. Security camera footage is one example. Does footage of the front door constitute patron use? How about a camera recording the computer area? ALA provides guidelines around the use of these cameras, but what is captured on the camera could determine if the recording falls under the definition of patron use record.

And what about meeting rooms? The system logs might be considered patron use records, but does the actual meeting room schedule fall under the definition, or is it public record?

ALA does not have as much guidance about this question as they do with security camera footage. In both cases, legal staff can give you some advice as to what is and is not protected under Section 6267.

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

Both library websites and online vendor resources collect patron data. Libraries want to know how many people visit a certain page on the library website, but they might not be aware that their web analytics software – Google Analytics, in particular – is collecting patron personal information that is then used to track patrons across non-library websites. Vendors go beyond web analytic software to collect patron data through use of proxy services, third party integrations for authentication methods, user accounts, and so on. The sheer amount of data exhaust by using online services presents considerable challenges in respecting patron privacy.

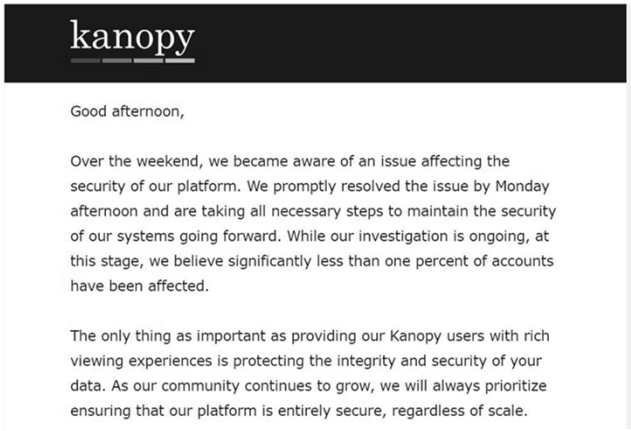
Patrons might not be aware about this data trail or of the extent of data collection from that trail. Public privacy notices set patrons' expectations around the library's practices around data collection and use. Another way patrons create expectations around the library's data practices is providing data for a specific use. Let's use signing up for a library card as an example. A person gives their name, age, and address to the library so they can use library services. What would happen, then, if they found out that the data was used for another purpose, such as being combined with an external data set that contains income level, education level, race/ethnicity, and gender identity to create segments for targeted marketing?

If you don't communicate about how the data will be actually used, patrons are less likely

to trust the library with their data.

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.


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.

And that was just expectations between the library and patrons! What about patrons' expectations around libraries' relationships with vendors? Vendors have multiple ways of collecting patron data, including direct collection from patrons. Libraries can give over more information about patrons than what is absolutely needed to use the vendor product. This is particularly important to be cognizant of when working with vendors who might request data beyond the minimal data needed to launch the service.

Vendors also communicate privacy to patrons, but in ways that can leave the library out of the conversation. On the slide is an example of when a vendor, Kanopy, directly contacted users about a data breach. Kanopy did not contact the libraries until days later, leaving library workers confused when patrons started contacting libraries about a breach that they didn't know about, and didn't know what to do about it. Kanopy is also an example of vendors using patron data for questionable purposes, with Kanopy directly emailing patrons when major library systems were considering not renewing their contract with Kanopy.

Be aware that vendors might engage in deceptive patterns that create confusion around privacy settings and information, making it difficult for users to have that control. Making a privacy notice hard to locate or navigate is one pattern, while confusing designs over buttons and toggle switches that don't clearly indicate if a privacy setting is enabled or not is another

example of deceptive patterns at work.

Libraries can help patrons navigate vendor privacy practices through a variety of platforms, including detailing how libraries work with vendors in protecting data privacy in the privacy notice and creating a page with key information about each vendor's privacy policy and practices.

[Image description: A letter from Kanopy to Kanopy users about a data breach.]

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

This leads us to patron communications!

A library must, 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 main privacy policy, but privacy notices need to be written for the general public about how the library goes about privacy in daily operations. They should explain, in the major languages of the service population, the patron's right to privacy and confidentially in their use of the library. The Toolkit section Operationalizing Privacy in the Library gives a list of what should be included, so I recommend going through those resources, as well as the examples in the training handbook for the companion training workshop, for more information and guidance around privacy notices.

You can use existing communication lines to inform patrons of privacy updates, such as library newsletter updates, blog posts, and press releases. You can use website alerts and pop ups for major updates, but research has shown that these can backfire if not used judiciously and not carefully designed.

One communication line that can help with addressing specific privacy issues is working with community partners and organizations. These real world relationships can reveal concerns that data wouldn't have shown. This dialogue between the library and the community can also be an opportunity to learn more about the privacy needs of patrons, which then the library can accommodate and meet those needs through programming and services.

Patron Privacy Programming and Services

- Digital literacy
- Information security and privacy
- Device security

There is already some really good examples of patron privacy programming, and I highly encourage that you take some time to study them and take notes about what you like. An example is the Cybersecurity Training for Youth Using Minecraft project, available on the PLP website. Other examples are listed in the last section of the Toolkit.

You can approach privacy programming in at least three ways. Many libraries offer some form of digital literacy programming. Digital privacy and security are key components in these classes. You can also have classes dedicated to information security and privacy. While other classes can give patrons “just in time” information for the specific topic being covered, 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.

Another opportunity for patron privacy programming is when patrons ask question about digital device troubleshooting and security, including smartphones, ereaders, and tablets. These one-on-one consultations are an opportunity for library workers to provide “just in time” privacy and security instruction or information about the specific device to patrons. Staff can also create a small flyer for patrons to take with them, as well as information about where they can learn more about privacy and security for their device.

[Image description: A group of four Black adult women gather around a desktop computer. Two are sitting in front of the computer, while one woman leans over to assist one of the sitting women, with the fourth woman standing off to the side looking on. Two other white adults are talking to each other in the background.]

[Image source: https://www.flickr.com/photos/kl/2544120735/ (CC BY SA 2.0)]

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

These programming options can be a part of a larger set of patron privacy services and programs. This patron privacy as a service can take the form of online and in person services. San Jose PL's Virtual Privacy Lab is an example of an online self-paced service that patrons can get a customized toolkit based on their needs. This toolkit covers common privacy topics and provides resources and in-depth discussions to cater to a range of patron skill and knowledge levels.

Cornell University Libraries' privacy services are another approach to patron privacy services where the emphasis is on privacy literacy instruction and one-on-one consultation on specific privacy risks and questions. These services plus other are listed in the last section of the toolkit, and I highly recommend checking them out for ways you can incorporate both self-paced and synchronous instruction and consultations.

Questions and Open Discussion

Wrap Up

Next Week

Week Four - Building and Fostering a Culture of Privacy

- April 28th, 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

Thank you

:-)

LDH Consulting Services

Becky Yoose
Library Data Privacy Consultant
LDH Consulting Services

Email:
becky@ldhconsultingservices.com

Resources and Further Reading

Additional bibliographies and resources can be found in the Toolkit and training resources at the https://www.plpinfo.org/dataprivacytoolkit/.