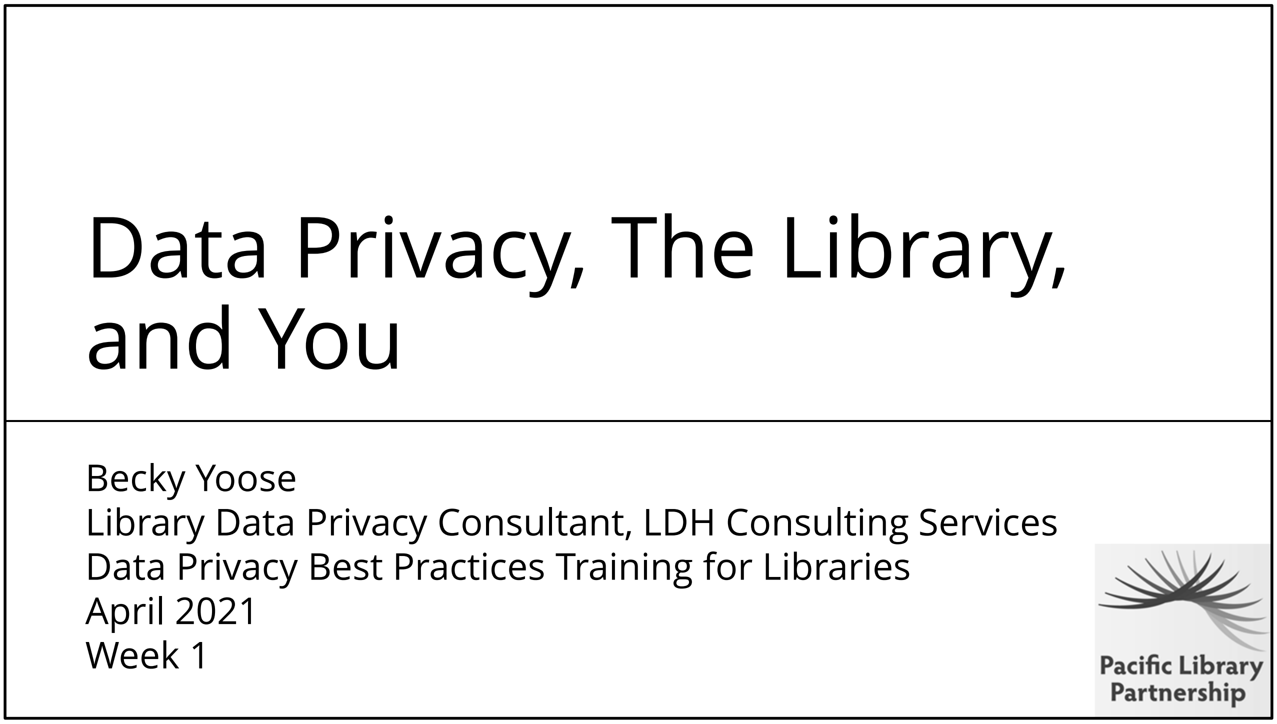
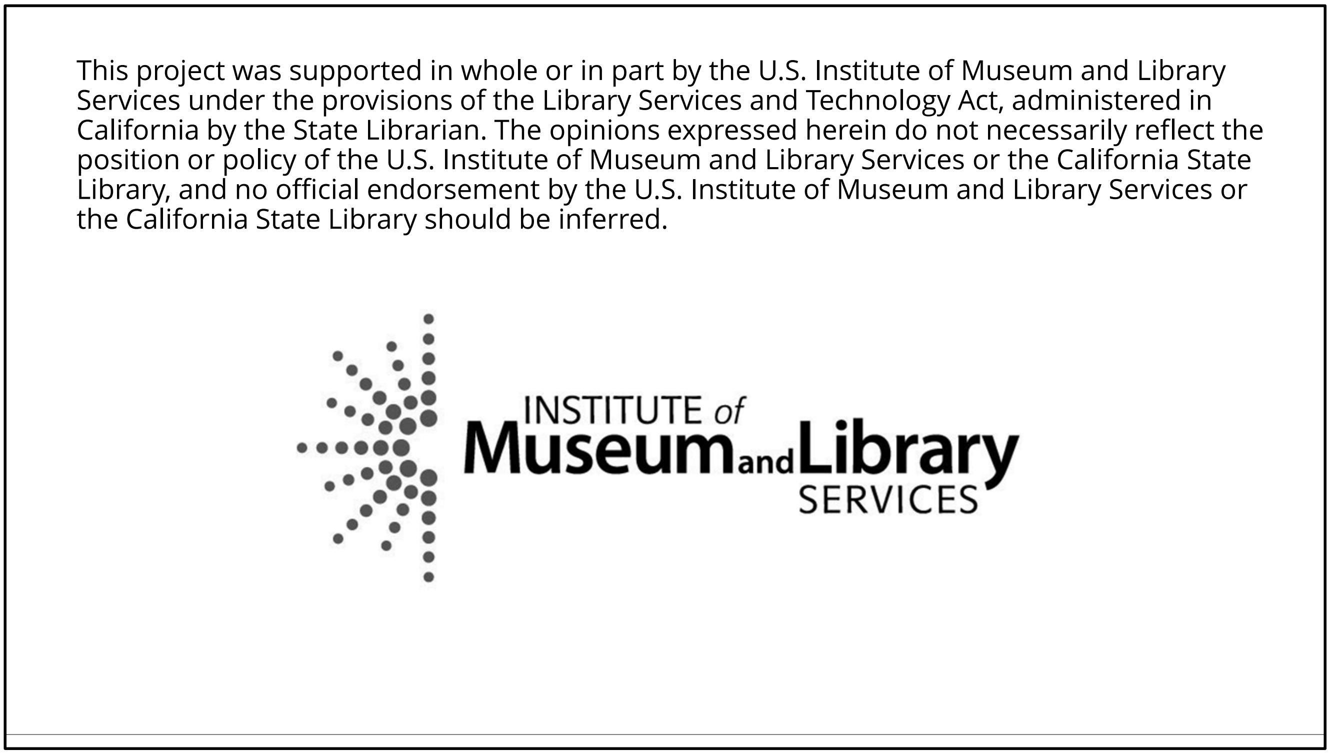


Data Privacy, The Library, and You

Becky Yoose
Library Data Privacy Consultant, LDH Consulting Services
Data Privacy Best Practices Training for Libraries
April 2021
Week 1

Pacific Library Partnership

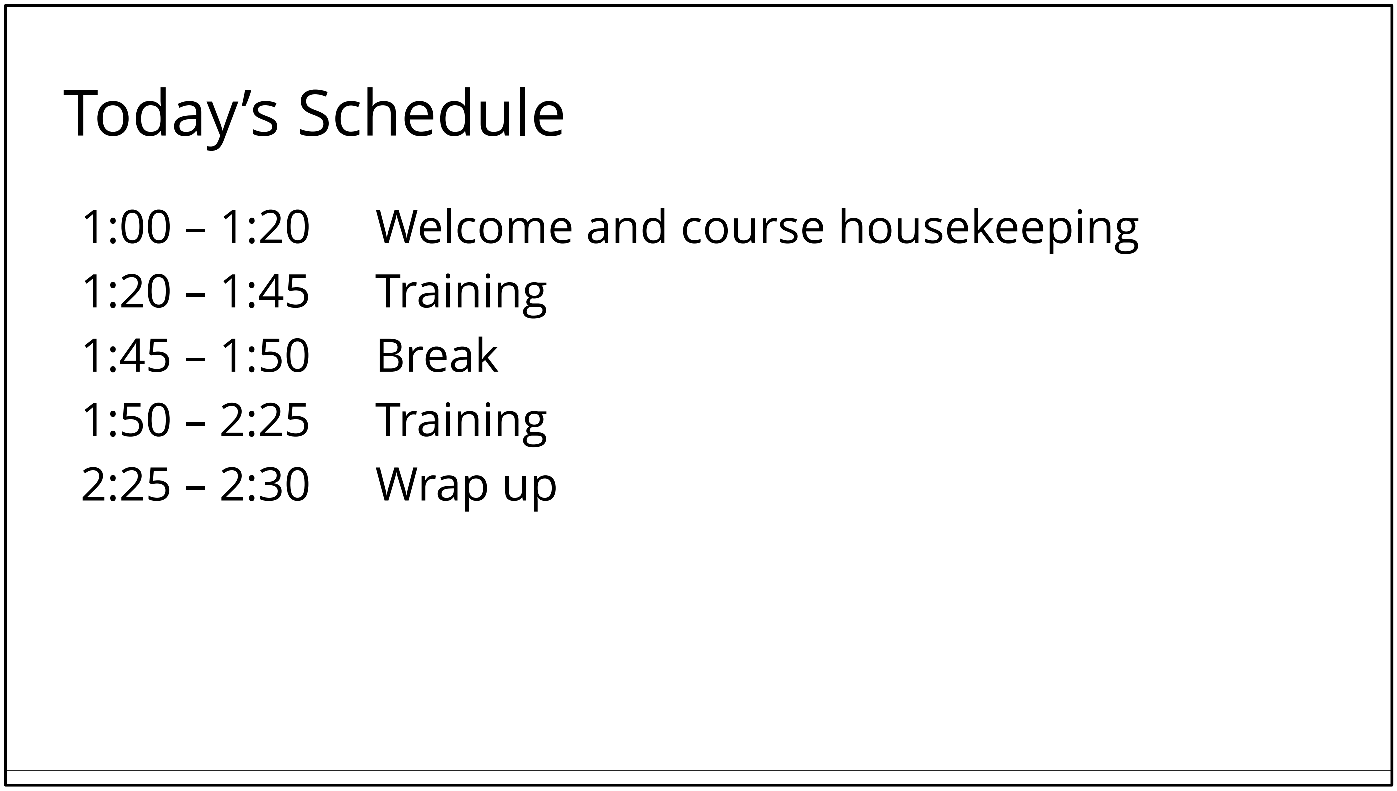
Welcome to the first week of the Data Privacy Best Practices Training for Libraries! I'm Becky Yoose, I use she/her pronouns, and I'm the founder of and Library Data Privacy Consultant for LDH Consulting Services.



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.

INSTITUTE of Museum and Library SERVICES

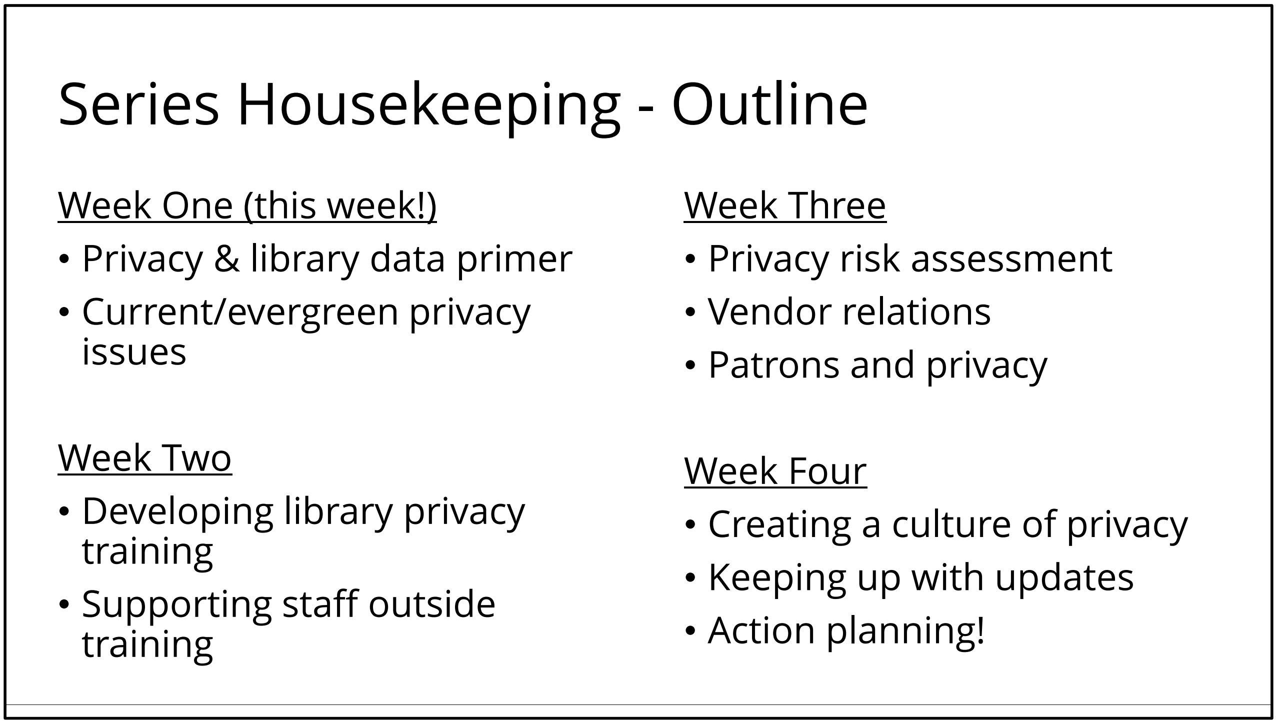
This is a quick FYI that this workshop is part of a project supported by the Library Services and Technology Act, so thank you to the grant authority for providing resources for this project. You can find this statement in the slide handouts as well.



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

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.



Series Housekeeping - Outline

Week One (this week!)

- Privacy & library data primer
- Current/evergreen privacy issues

Week Two

- Developing library privacy training
- Supporting staff outside training

Week Three

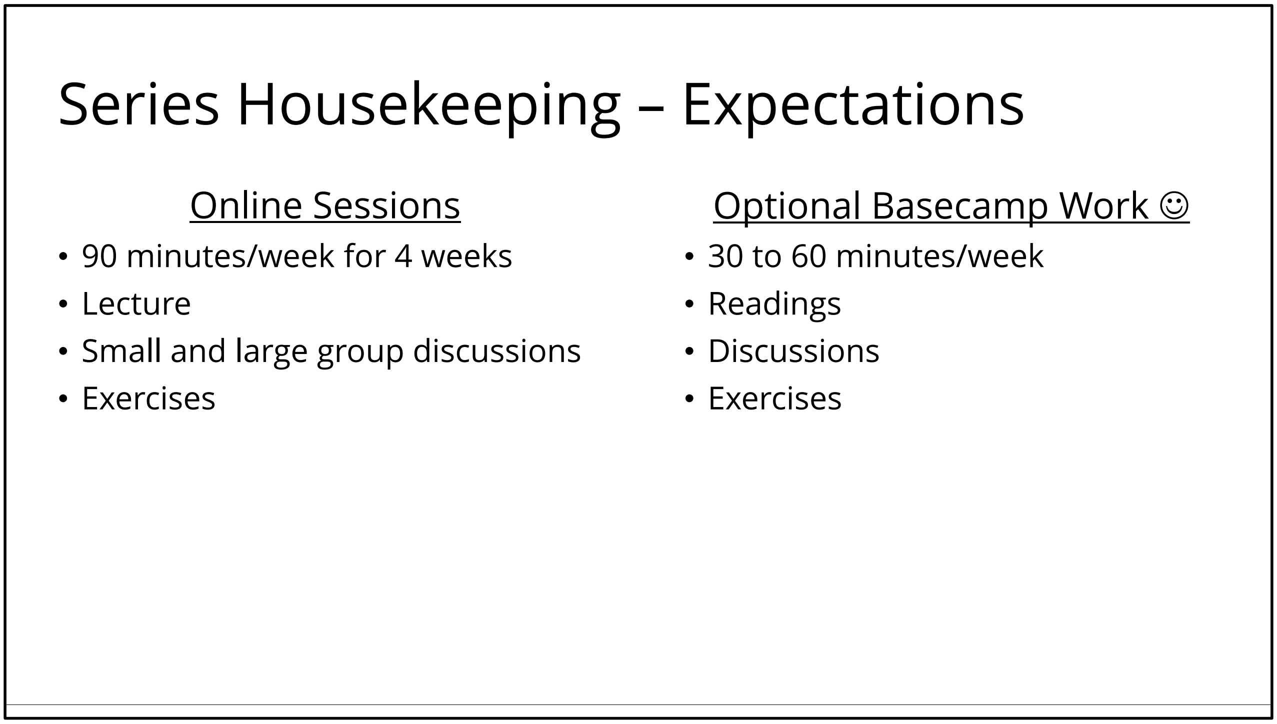
- Privacy risk assessment
- Vendor relations
- Patrons and privacy

Week Four

- Creating a culture of privacy
- Keeping up with updates
- Action planning!

This series builds off of the training conducted in early 2020. I highly recommend taking some time to review the training materials if you haven’t already done so.

This week we are starting off with an overview of libraries and data privacy. For those of you who too last year’s training, this should be a refresher. Week two is where we get into library privacy training, including training development and ways of supporting staff outside of training. Week three goes back into library operations with three main topics that go beyond basic data privacy training, including risk assessment and patron programming. Week Four brings everything together to focus on building a culture of privacy in all areas of the library, including what to do after the series.



Series Housekeeping – Expectations

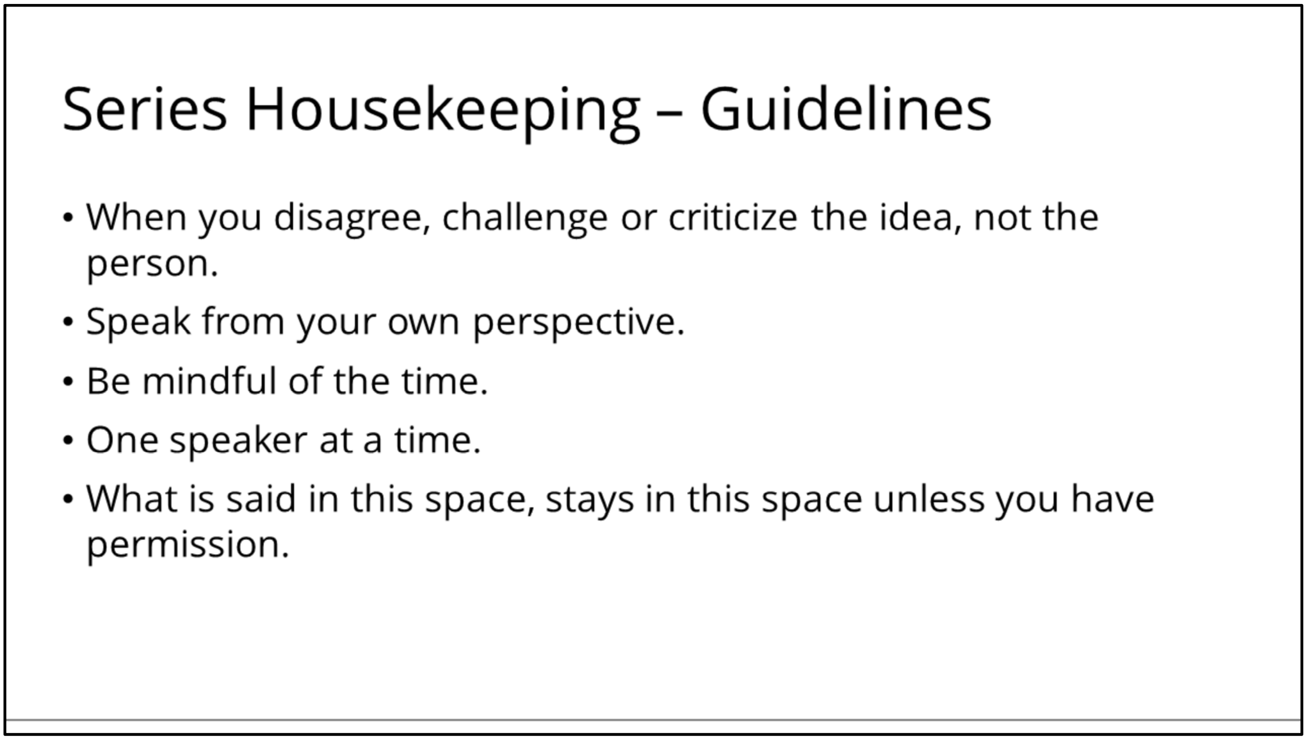
Online Sessions

- 90 minutes/week for 4 weeks
- Lecture
- Small and large group discussions
- Exercises

Optional Basecamp Work ☺

- 30 to 60 minutes/week
- Readings
- Discussions
- Exercises

The online sessions will be a mix of lecture, discussions, and exercises. In addition to the sessions, there will be some optional readings and exercises on Basecamp. These will build off of the topics covered in the online sessions, and should take about 30 to 60 minutes a week.

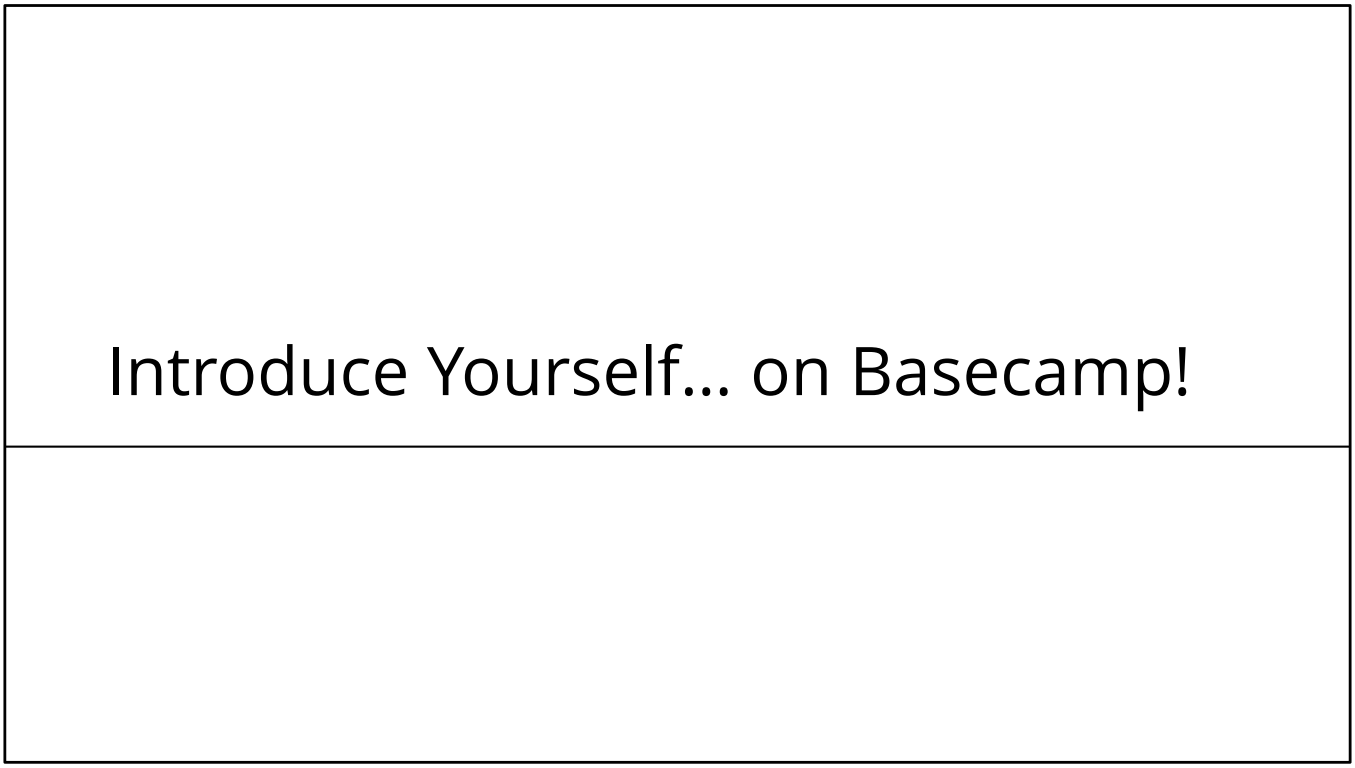


Series Housekeeping – Guidelines

- 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.

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

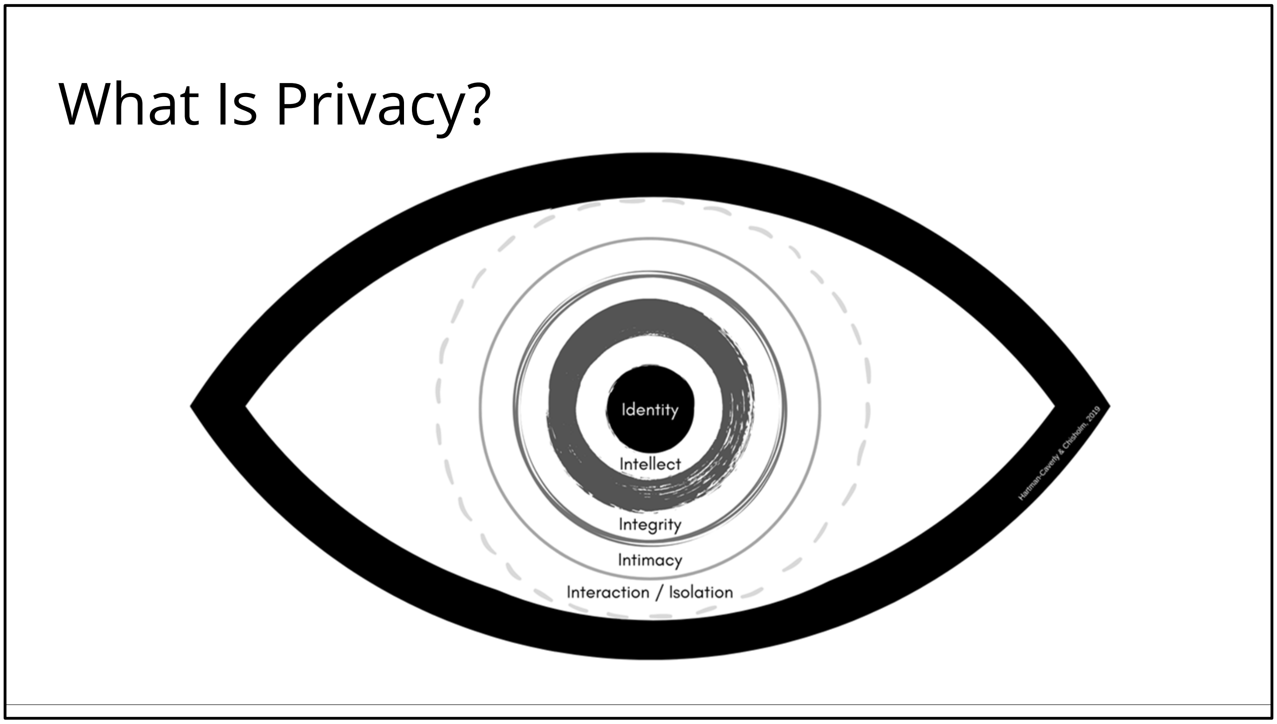
- When you disagree, challenge or criticize the idea, not the person.
- Speak from your own perspective. "I" statements are useful ways for keeping from generalizing about what others think or feel.
- We'll have some time for discussion, but it's always helpful to be mindful of the time while you are 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.



Introduce Yourself… on Basecamp!

1. Starting From The Top – Privacy Fundamentals

Thank you everyone! Let’s start from the top and talk about what we mean when we talk about privacy.



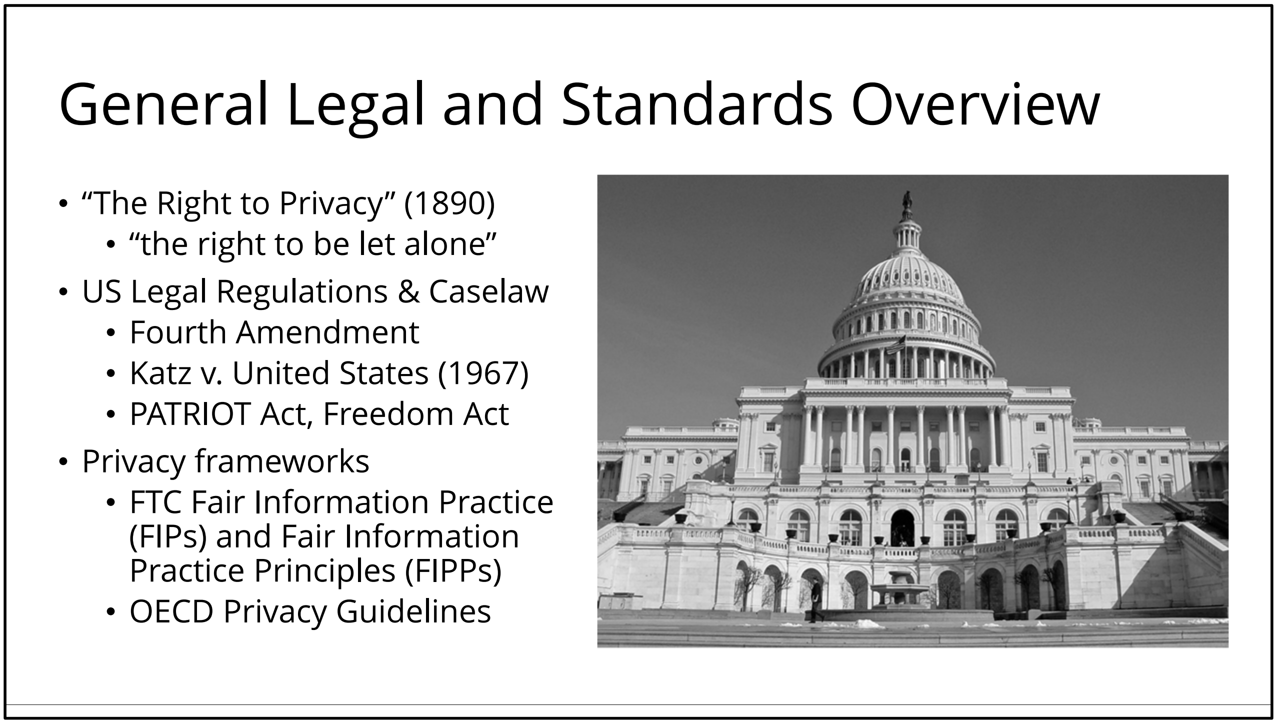
What Is Privacy?

Hartman-Caverly & Chisholm, 2019

Privacy means many things to many people. There are different types of privacy – for example there is information privacy, or the privacy of personal information such as medical or financial records, but there is also bodily privacy, which refers to the privacy of the physical body, such as genetic information and certain actions or choices that the person makes about their physical body. We all might have these types of privacy in our definition, but these definitions might change based on the context of the question or the setting in which the question is asked. We might have different definitions for privacy if we're asked to define the term for ourselves and in our professional work.

The many facets of privacy can make it difficult to find common ground when discussing privacy with others. There are a couple of frameworks and models you can use to create a starting point when discussing privacy with others that takes into account these facets. Librarians Sarah Hartman-Caverly and Alexandria Chisholm created the Six Private I's as a conceptual framework in an attempt to represent the various layers or zones in which privacy protects: identity, intellect, bodily/contextual integrity, intimacy, and interaction and isolation. This framework covers the main facets of the types of privacy people encounter in their daily lives, and could be used to tie these facets together with regards to their relationships with each other.

[Image description: A drawn black and white clipart human eye with six labeled ring areas. Starting from the center circle going out: Identity, Intellect, Integrity, Intimacy, and Interaction/Isolation.]
[Image source: https://sites.psu.edu/digitalshred/2020/10/01/six-private-is-privacy-conceptual-framework-hartman-caverly-chisholm/ CC-BY-SA-NC licensed (with attribution to Sarah Hartman-Caverly and Alexandria Chisholm)”]



General Legal and Standards Overview

- “The Right to Privacy” (1890)
  - “the right to be let alone”
- US Legal Regulations & Caselaw
  - Fourth Amendment
  - Katz v. United States (1967)
  - PATRIOT Act, Freedom Act
- Privacy frameworks
  - FTC Fair Information Practice (FIPs) and Fair Information Practice Principles (FIPPs)
  - OECD Privacy Guidelines

Privacy as we know it is heavily influenced by external factors, such as legal regulations and professional/industry standards. The legal right to privacy has evolved through legal opinions, regulations, and caselaw. “The Right To Privacy”, published in 1890 in the Harvard Law Review, states that individuals have “the right to be let alone”. This law review article became one of the greatest influencers of US privacy regulations. The Choose Privacy Every Day blog has a series of posts around US privacy law, including an post about “the Right To Privacy” that I recommend if you want a detailed analysis.

The Fourth Amendment of the Bill of Rights is a key component in privacy regulations and cases. The text itself is short: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

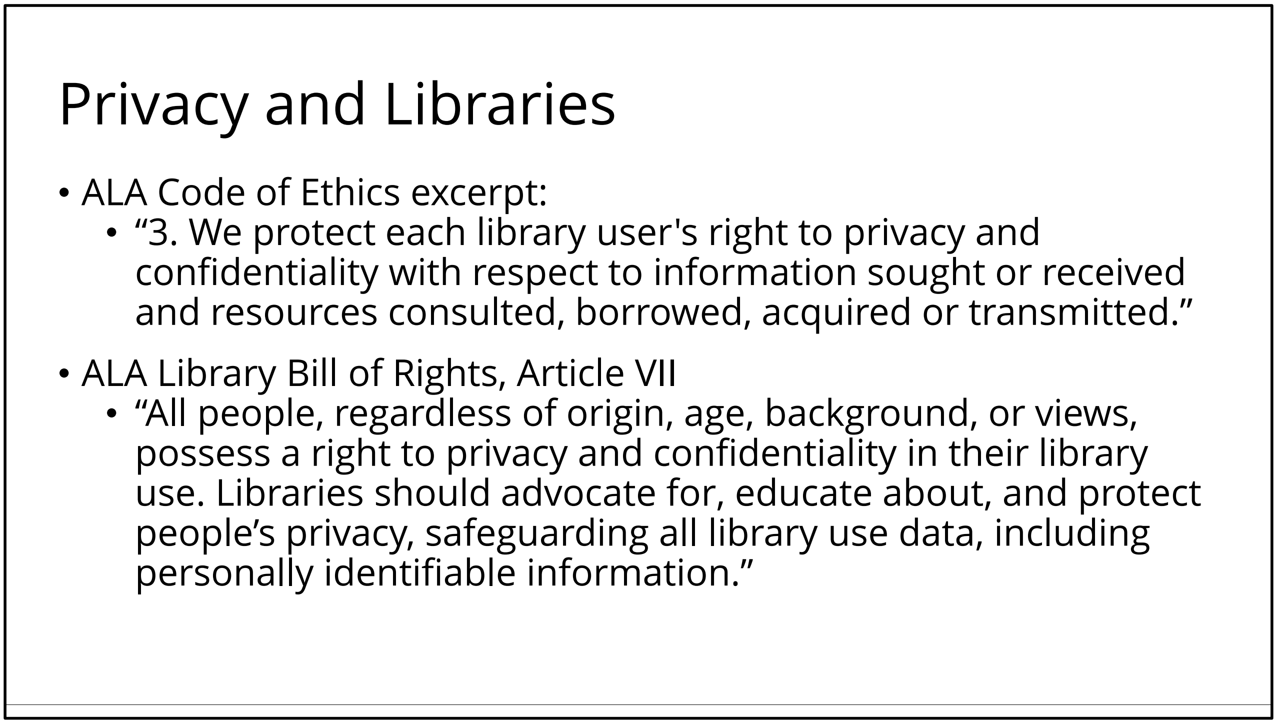
The interpretation of the Fourth Amendment plays a pivotal role in privacy cases, such as the Katz v. United States in 1967, where the Supreme Court expanded the amendment’s protections in their ruling, stating that the amendment grants people a reasonable expectation of privacy even in public spaces. However, this interpretation has not stopped legislation that would be considered by some to be a violation of a person’s right to privacy, including the PATRIOT Act in 2001 and the subsequent Freedom Act in 2015 that allowed for government agents to conduct warrantless searches of “tangible things” which includes library records.

On top of legal regulations and caselaw, the definitions of privacy are also shaped by standards and frameworks. The FTC Fair Information Practice Principles created in the 1970s had five principles:

- Consent
- Notice
- Access
- Integrity
- Enforcement

These five principles were expanded to eight in the OECD Privacy Guidelines. We won’t cover these frameworks in depth in this session since they were covered in the trainings in 2020, but it is good to be aware that these frameworks have influenced how privacy is approached by industry and regulations throughout the years.

[Image description: The West front of the US Capital building.]
[Image source: https://www.flickr.com/photos/schuminweb/50178344916/ (CC BY SA 2.0)]

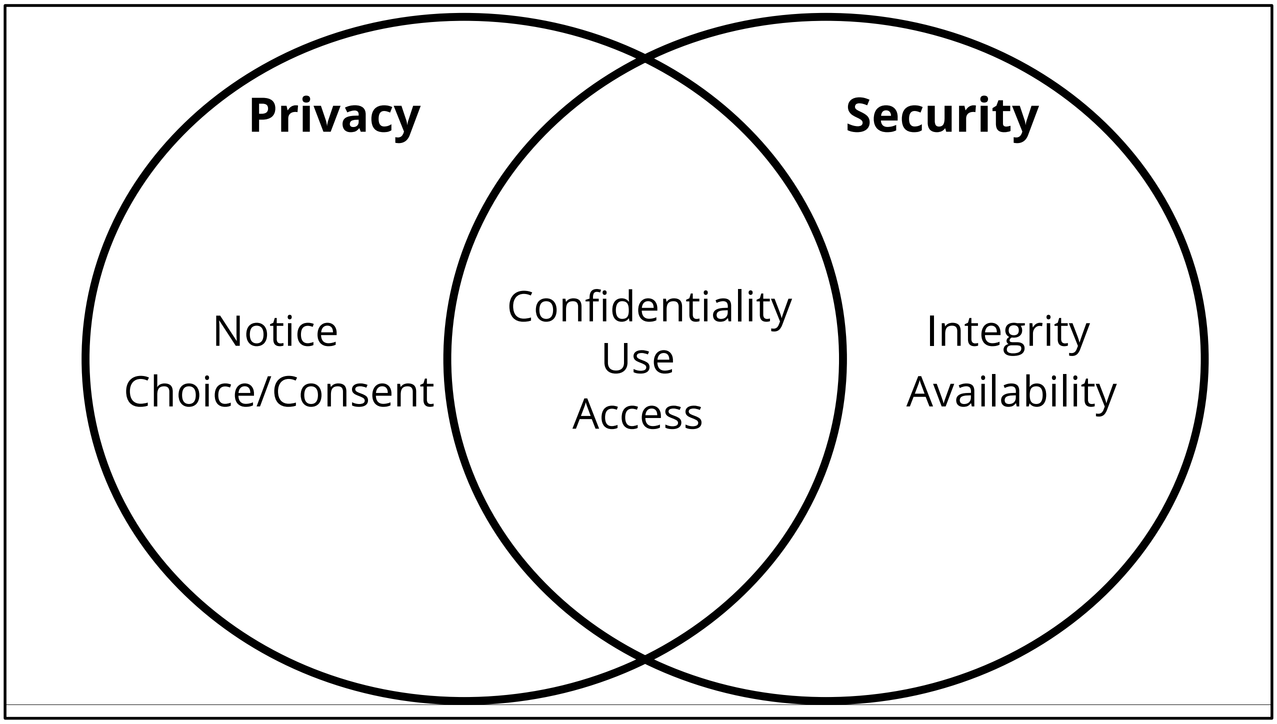


Privacy and Libraries

- ALA Code of Ethics excerpt:
  - “3. We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted.”
- ALA Library Bill of Rights, Article VII
  - “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.”

The library profession also shapes our individual definitions of privacy. The definition of privacy relates to patrons and their relationship to the library. ALA’s code of ethics charges library professionals to protect the information surrounding patron use of library services and resources, and the library bill of rights gives patrons the right to privacy when using the library. The bill of rights reinforces the charge from the code of ethics of the library to protect patron use data. Privacy is argued as one of the core tenants of Intellectual Freedom in the sense that a patron is not able to make full use of the library resources if they know that they will face consequences based on the subjects or types of resources they use.

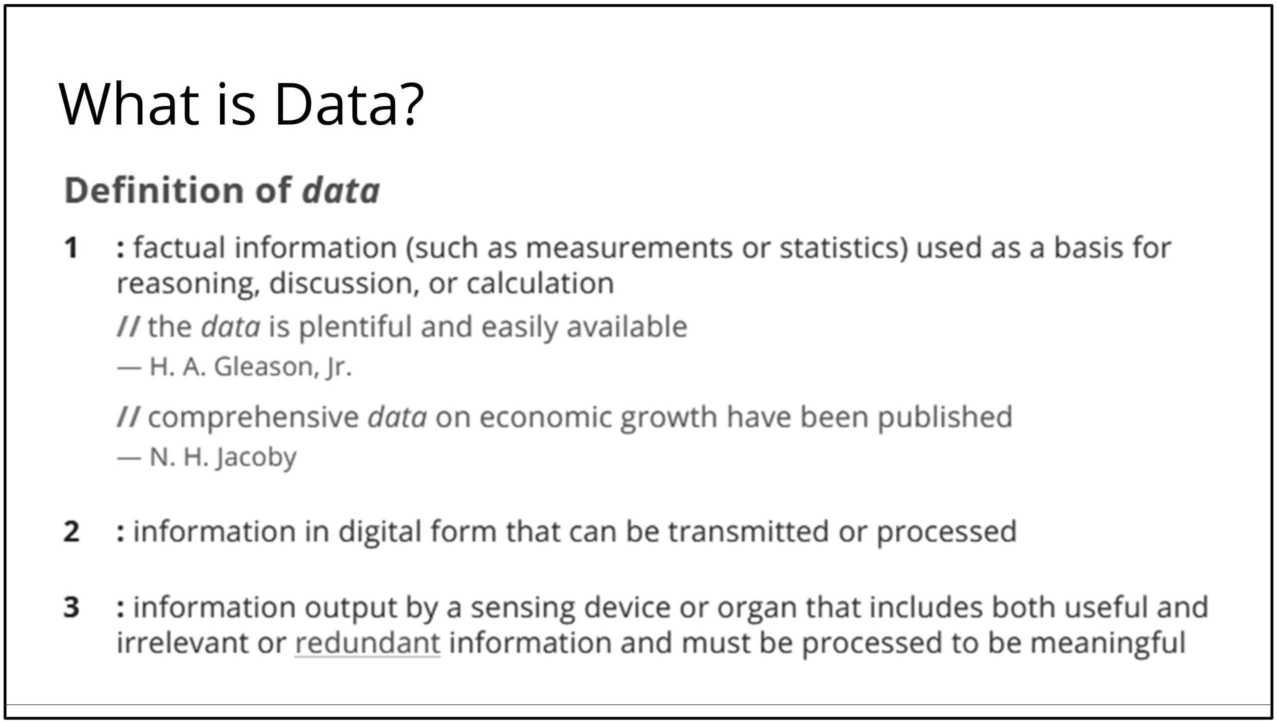
One thing I want to point out is that both documents mention privacy and confidentiality. This is an important distinction, particularly when we define privacy in relation to how the information is treated. While privacy is a right from intrusion, confidentiality means that the information given to a party will not be disclosed to unauthorized third parties. That’s a bit of an oversimplification, but it should give you a sense that these two concepts are distinct even though there is some overlap.



This overlap also happens when we talk about privacy and security. While privacy and security share some core tenants, such as confidentiality, use, and access of information, ultimately the two are not the same. Security pertains to protecting a set of assets, be it property, information, or persons. Privacy centers around the collection, use, disclosure, and retention of assets, emphasizing the roles consent and notice in those processes.

There is a popular saying in the privacy profession – “You can have security without privacy, but you cannot have privacy without security.” Security can tell you how to protect the data that you have, but privacy will ask you if this data should be collected and retained in the first place. Security is still important, though! The security companion course to the privacy train the trainer course is essential in protecting the privacy of your patrons, focusing on how library and patron data can be compromised by internal and external threats and vulnerabilities.

[Image description: A Venn diagram showing two circles "Privacy" and "Security" overlapping with each other. The overlapping area contains "Confidentiality, Use, Access". The Privacy circle contains "Notice, Choice/Consent" and the Security circle contains "Integrity, Availability“.]



What is Data?

Definition of *data*

1 **:** factual information (such as measurements or statistics) used as a basis for reasoning, discussion, or calculation

// the *data* is plentiful and easily available
— H. A. Gleason, Jr.

// comprehensive *data* on economic growth have been published
— N. H. Jacoby

2 **:** information in digital form that can be transmitted or processed

3 **:** information output by a sensing device or organ that includes both useful and irrelevant or redundant information and must be processed to be meaningful

Now that we established what we mean when we talk about privacy, it’s time to shift our attention to explore what we mean when we talk about data. We’ll start with this definition from Merriam Webster, where data is one of three things:

1. Factual information
2. Digital form of information
3. Information output that has to be processed before it can become meaningful

Some of us might also remember the DIKW hierarchy where data is at the bottom of the pyramid waiting to be processed into the next level of information. Both of these definitions, however, don’t capture the complexity of data. Data is not just some raw and unrefined resource to be processed into meaningful information. Data is much more than that.

[Image description: Definition of data from Marriam Webster online dictionary. Summary of three definitions:
1. Factual information
2. Digital form of information
3. Information output that has to be processed before it can become meaningful

]
[Image source: https://www.merriam-webster.com/dictionary/data]

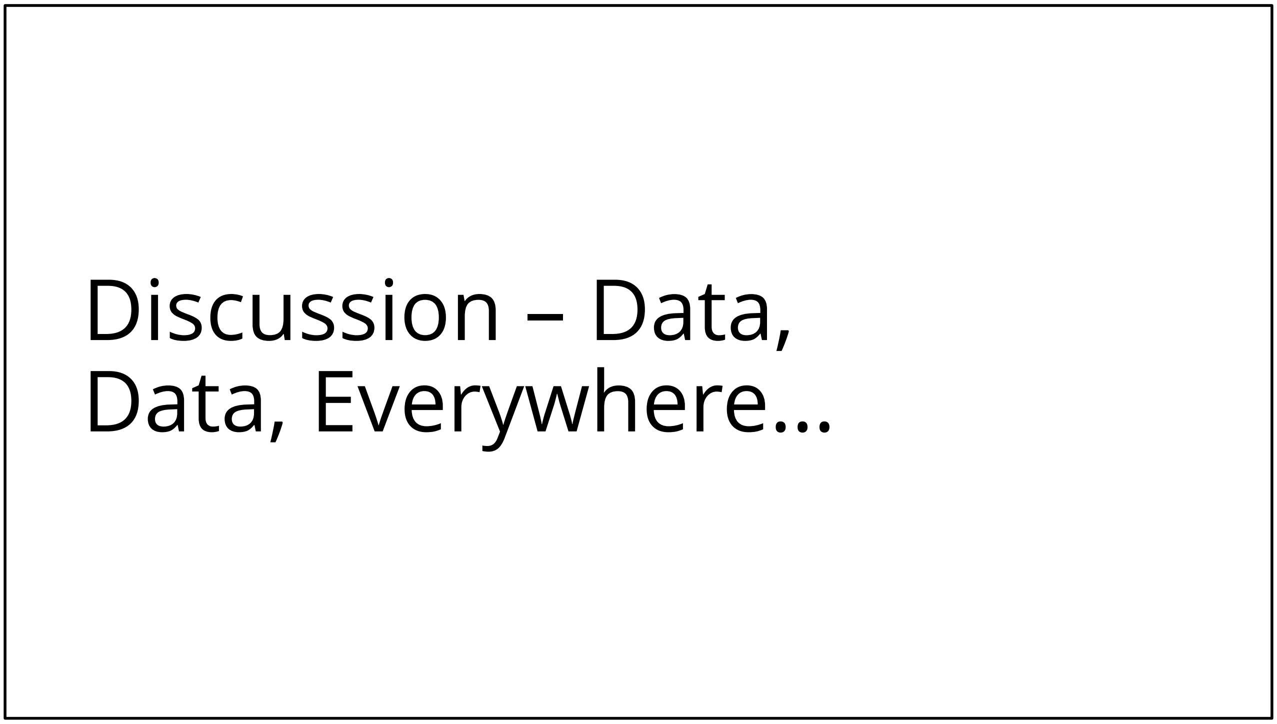
We create data.

We are data.

We create data in our everyday life. Many of our devices generate data when we use them, including the increasing number of IoT. We generate data when we pay for goods and services, walk in a store generates data through security cameras, door counters, beacons that search for your mobile device's Bluetooth or wifi connections. We generate data by walking past our neighbor's house that has a Ring camera on the front door. We generate data while we work our 9-5 jobs.

Some of this data is needed for operational purposes – the credit card company needs information to process the payment, for example. However, a lot of the data we generate is data exhaust that could be collected and used by third parties without prior consent or awareness from the people generating that data. This trail of data reveals who we are in terms of our behaviors, interests, and habits. It's near impossible to separate the person from the data they generate. Even when we talk about aggregation of data, or when we describe data through metadata, we can still get a relatively accurate picture of the person generating the data.

Privacy is more difficult to achieve with the shift of everyday life to rely on technologies that collect data on almost all the zones we encountered in the Six Private I's framework. When we talk about data privacy we need to acknowledge that we are not only protecting informational privacy, but ourselves as a whole. In essence, we are data and our approach to data privacy needs to reflect that.



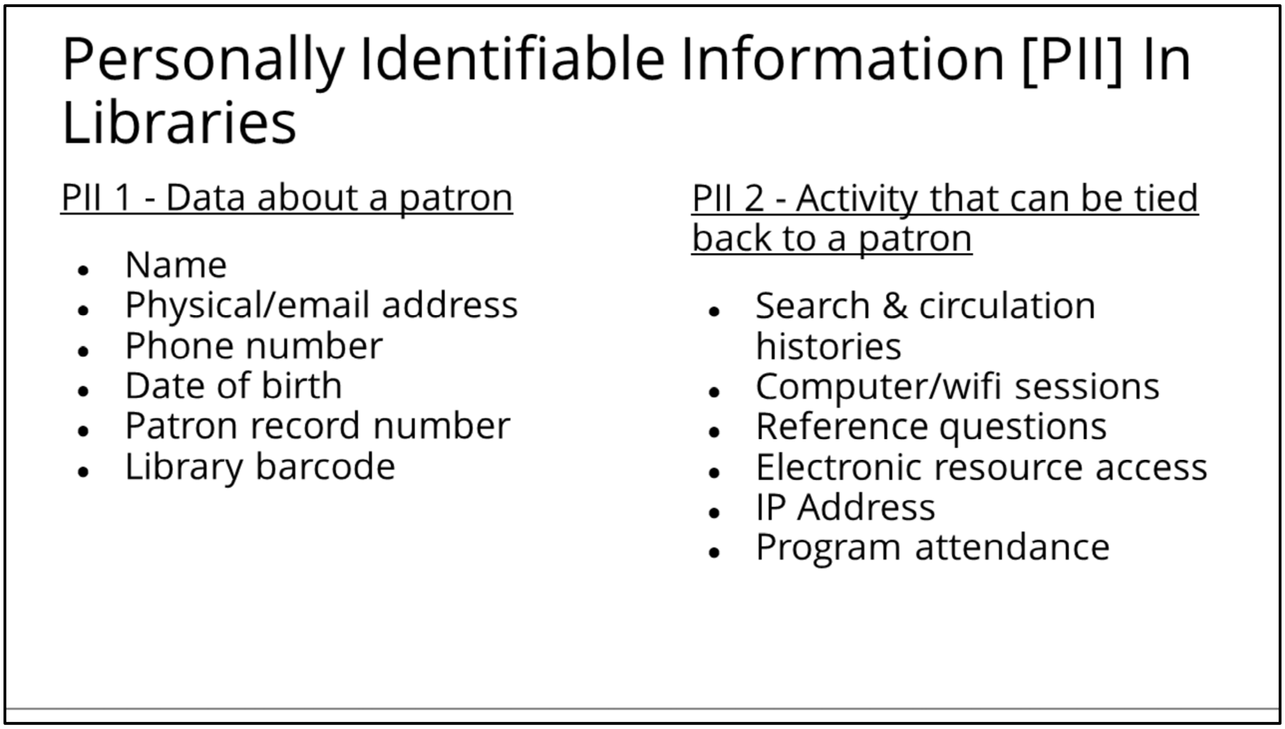
Discussion – Data, Data, Everywhere…

Discussion prompt – How do you currently approach privacy with your everyday life and data?

Additional prompt – What changes would you make if you had the time, knowledge, and resources?

2. Library Patron Data Privacy Fundamentals

Alright! Libraries are not immune from data exhaust. So it’s time to talk about the fundamentals of data privacy in libraries.



Personally Identifiable Information [PII] In Libraries

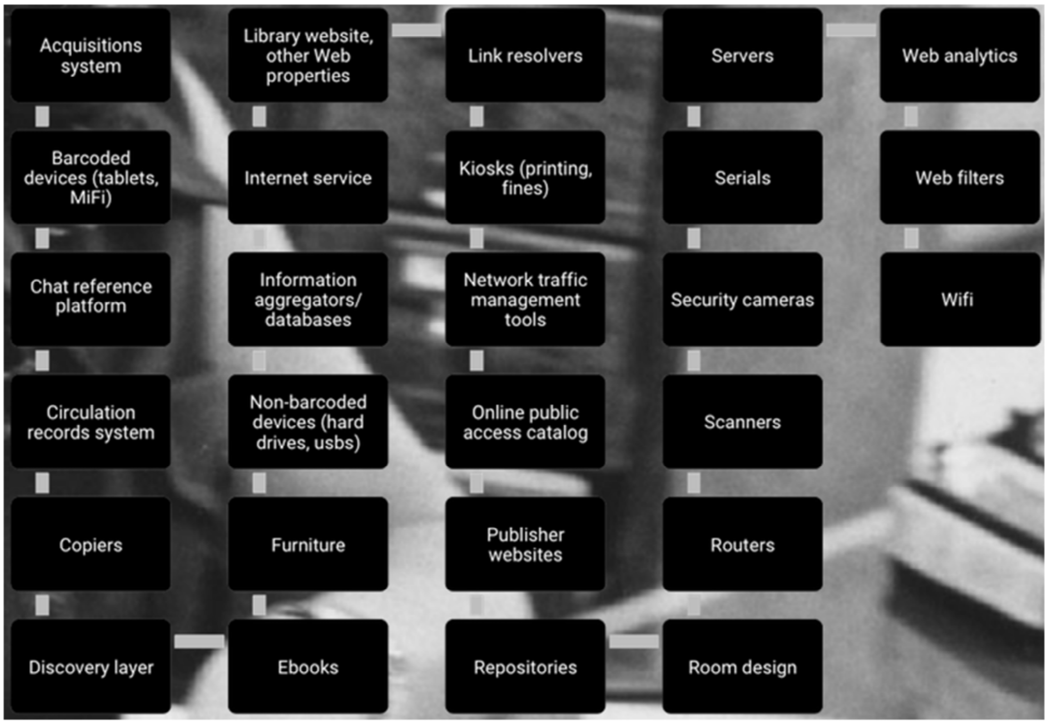
PII 1 - Data about a patron

- 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

The patron data that libraries have can be divided into two types of Personally Identifiable Information or PII. The National Institute of Standards and Technology splits PII into two categories – data about you, and data that is linked to you. PII-2 data can be used in certain circumstances to reverse engineer an identity. For example, I might not know your name, but if I have access to your Google search history, I can narrow down or even determine precisely who you are.



Acquisitions system

Barcoded devices (tablets, MiFi)

Chat reference platform

Circulation records system

Copiers

Discovery layer

Library website, other Web properties

Internet service

Information aggregators/ databases

Non-barcoded devices (hard drives, usbs)

Furniture

Ebooks

Link resolvers

Kiosks (printing, fines)

Network traffic management tools

Online public access catalog

Publisher websites

Repositories

Servers

Serials

Security cameras

Scanners

Routers

Room design

Web analytics

Web filters

Wifi

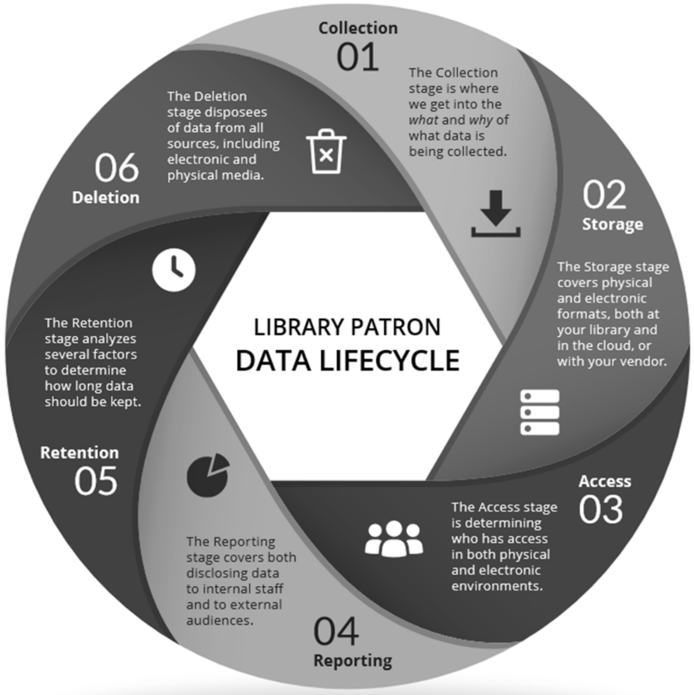
Your library collects a lot of data about your patrons. The slide shows a screenshot of a generic library's physical and online environments. With the exception of a couple of items, the majority of items listed on the slide collect, store, and share patron data in one way or another. Your library's integrated library system is the main database for patron data - name, address, age - but other systems collect and store patron data, such as your catalogs, discovery layers, and digital resources. Your physical environment also collect patron data, such as copiers, public computers, and devices that circulate, such as hot spots and laptops. This is either collected by the library or by a third party, be it a vendor or parent organization (university, city department, school, etc.).

This slide however doesn't capture everything. Take paper documents, for example. The paper forms located in staff file cabinets, desks, and recycling bins. This information might have already been entered into a secured electronic format, but what happens to the paper form after that?

We also can't forget about email. Staff send emails to other staff, patrons email staff, and staff email patrons. All these emails will have patron data that needs to be protected as well. Staff email also has the added complication that in the majority of libraries, staff email is subject to public records disclosure requests. Most likely you might have a chance to redact patron information before release, but that still doesn't account for staff use of this information in their inbox

[Image description: A series of black boxes listing software, systems, and physical components of a library that can determine what patron data is collected by the library.]

[Image source: https://dataprivacyproject.org/learning-modules/historical-overview/#privacychallenges2]



LIBRARY PATRON DATA LIFECYCLE

Collection 01

The Collection stage is where we get into the *what* and *why* of what data is being collected.

02 Storage

The Storage stage covers physical and electronic formats, both at your library and in the cloud, or with your vendor.

Access 03

The Access stage is determining who has access in both physical and electronic environments.

04 Reporting

The Reporting stage covers both disclosing data to internal staff and to external audiences.

Retention 05

The Retention stage analyzes several factors to determine how long data should be kept.

06 Deletion

The Deletion stage disposees of data from all sources, including electronic and physical media.

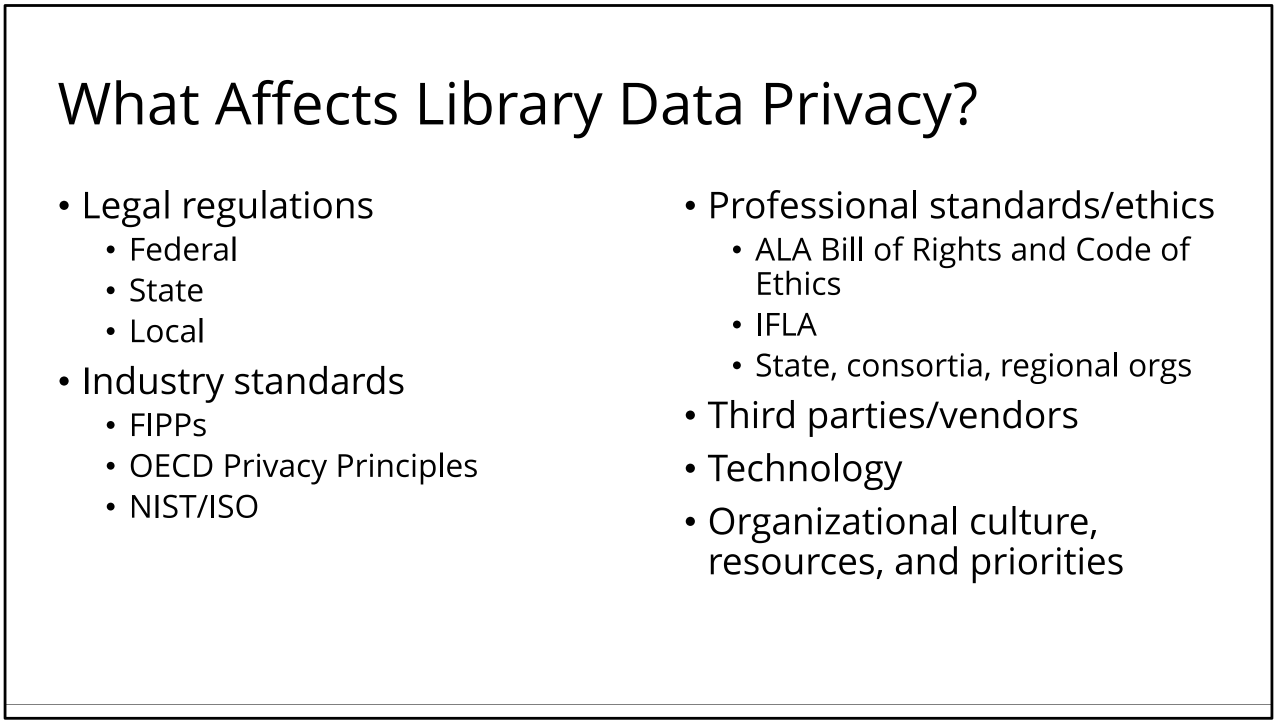
The patron data in the library goes through a lifecycle. There are six stages in the cycle: collection, storage, access, reporting, retention, and deletion. You might remember this from our patron data lifecycle workshop back in 2020! The lifecycle usually starts with collection and ends with deletion. There is some overlap between stages - for example, the access and reporting stages share the concern about who has access to what data used in both generating and publishing the report.

Each stage has a certain amount of risk attached to it. Let’s take collection for example. The data you decide to collect will determine the amount of harm incurred by both the patron and the library if that data is breached or leaked. Collecting driver’s license numbers in the patron record, for example, can put patrons at risk for identity theft if the data is improperly accessed by the public or by staff.

Libraries can create policies and procedures about data collection, storage, access, and retention for staff to follow. Going back to our collection example, we can mitigate risk through data inventories and limiting data collection to just data that is tied to a demonstrated business need.

Libraries have less control over data privacy when they are working with vendors. Sticking to the collection stage example, a vendor system might be collecting patron data that you have no clue that is being collected, and there might not be any indication in documentation or administration settings that this data is being collected. Not knowing what exactly is being collected by the vendor's system creates a unknown risk that is hard to mitigate. We'll talk more about vendors in Week Three.

[Image description: A circle flowchart depicting the patron data lifecycle. The lifecycle has six stages: collection, storage, access, reporting, retention, and deletion.]
[Image Source: Data Privacy Best Practices Toolkit for Libraries]



What Affects Library Data Privacy?

- Legal regulations
  - Federal
  - State
  - Local
- Industry standards
  - FIPPs
  - OECD Privacy Principles
  - NIST/ISO
- Professional standards/ethics
  - ALA Bill of Rights and Code of Ethics
  - IFLA
  - State, consortia, regional orgs
- Third parties/vendors
- Technology
- Organizational culture, resources, and priorities

The data in the lifecycle is affected by several factors, some of which contradict with each other, while others are absent all together depending on where the library is located.

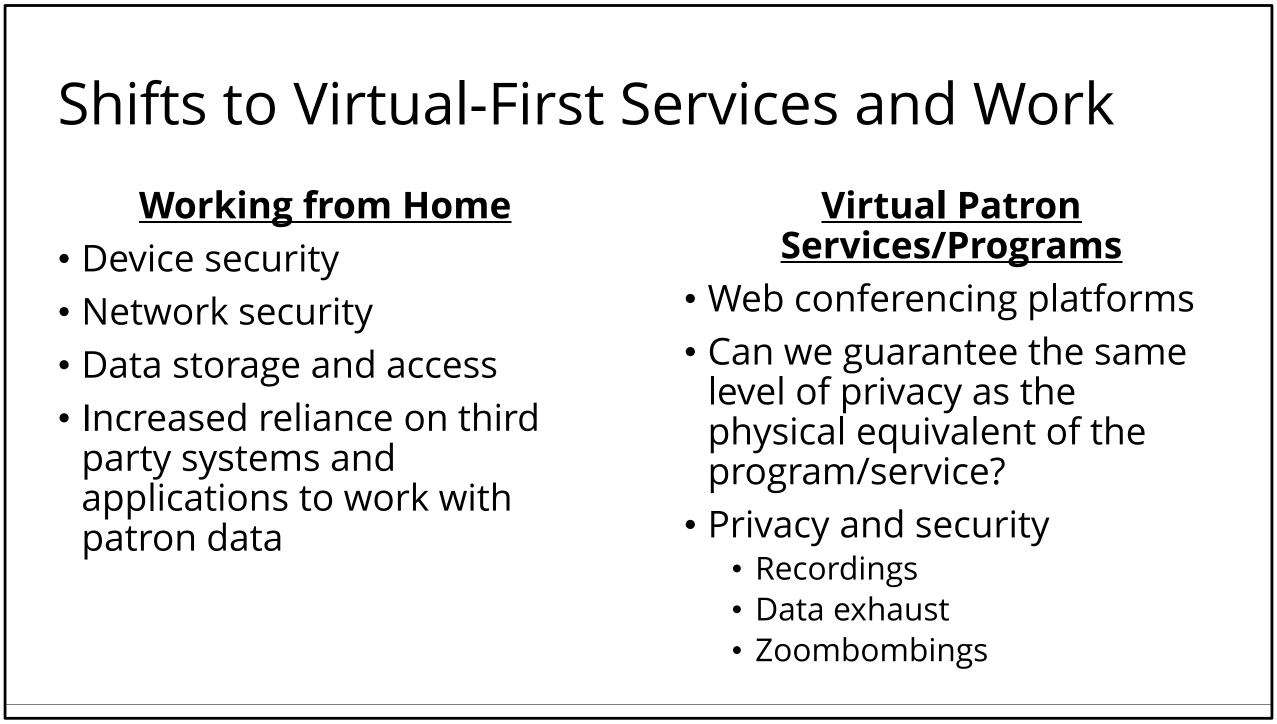
That’s the case with legal regulations. There is no one federal data privacy law, nor is there one library data privacy law. Instead, the US takes a sectorial approach to data privacy. Healthcare has the Health Insurance Portability and Accountability Act or HIPAA, educational institutions have the the Family Educational Rights and Privacy Act, or FERPA. Depending on the library these federal laws might apply to patron data privacy. Each US state addresses library privacy in state regulations or Attorney General statements, but there is no consensus as to what is protected. California, for example, has one of the most comprehensive library patron privacy laws in the country. California Government Code section 6267 states that any patron use records from any library that receives public funds shall remain confidential and not be disclosed except when a person is acting within the scope of their duties, you have written authorization from the patron, or by court order. This limitation on disclosure also pertains to any third party acting on behalf of the library, which includes library vendors. What also makes this Section strong is the definition of patron use records, which covers records that identify patrons as well as recorded transactions of a patron’s library resource use. However, California is the exception, and some states only allow exceptions from public disclosure of circulation records. On top of all of this are local regulations that could add protections around disclosure or provide retention schedules for certain records.

Industry and professional standards and ethics are also shapers of library policy and procedure. Our work with vendors also shape data privacy practices in the form of disclosure of patron data and the nature of the relationships we have with vendors and other third parties. In addition it’s hard not to ignore how the evolution of the use of technology in libraries has changed library’s approaches to data privacy throughout the decades.

However there are other factors that we might not be fully aware of in their effects on how libraries do privacy. Organizational culture and priorities can ultimately decide the effectiveness of data privacy practices at the library. We’ll be covering organizational factors in Week 4 in detail, but this is one factor that, if ignored, can reduce the effectiveness of any library privacy program or training.

3. Current/Evergreen Patron Data Privacy Topics

We’re on the home stretch! We covered the historical and foundations of data privacy in libraries, but the library is an evolving organism. With this evolution comes changing issues and challenges to data privacy. This section covers some of the current issues and challenges that libraries encounter with data privacy.



Shifts to Virtual-First Services and Work

Working from Home

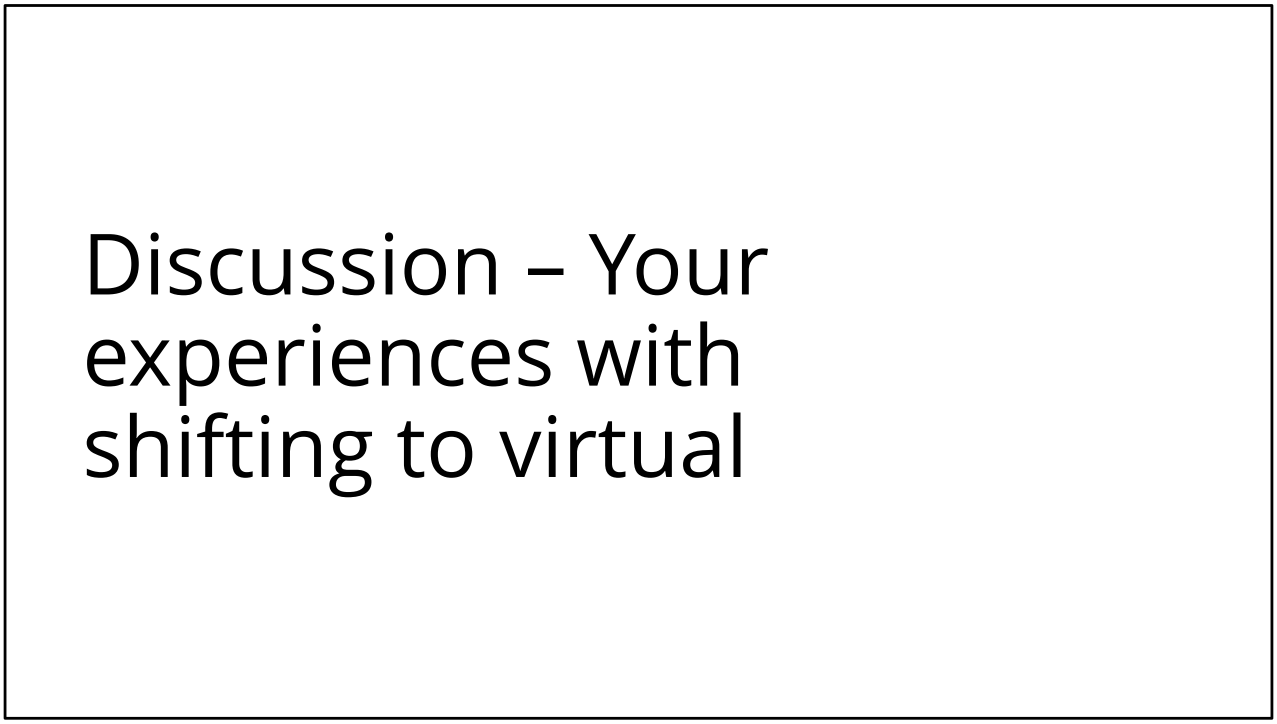
- Device security
- Network security
- Data storage and access
- Increased reliance on third party systems and applications to work with patron data

Virtual Patron Services/Programs

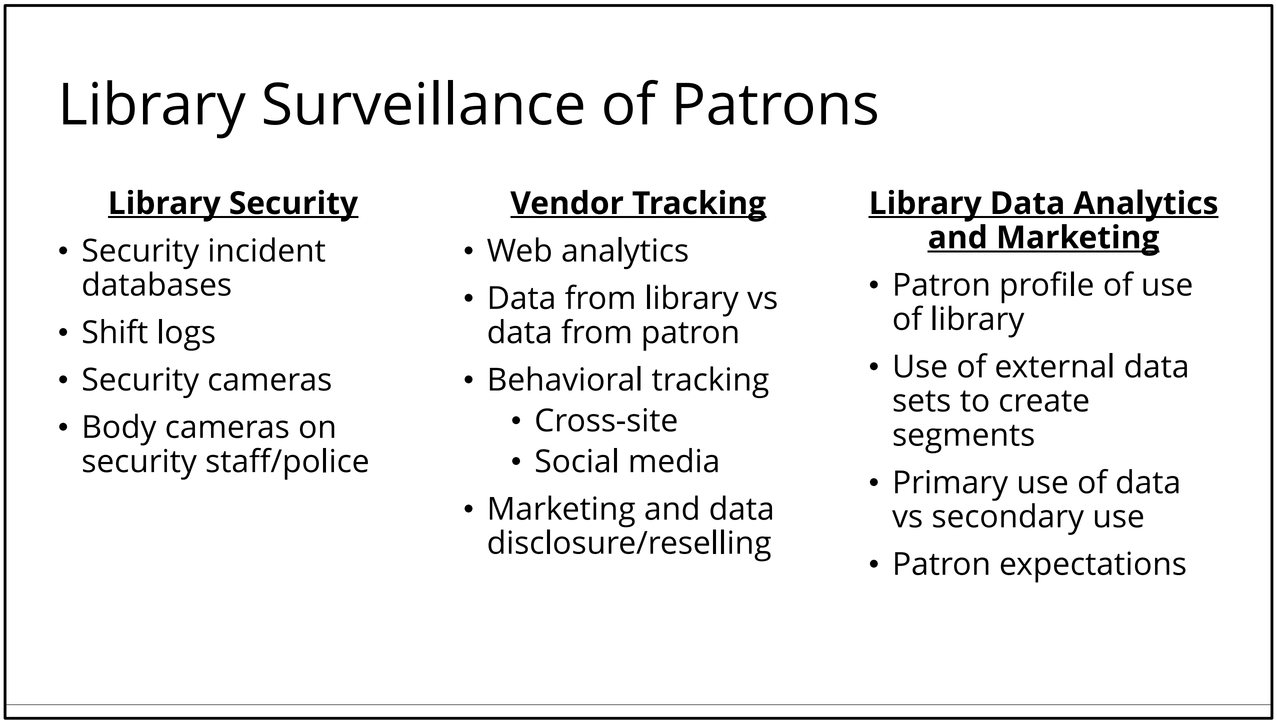
- Web conferencing platforms
- Can we guarantee the same level of privacy as the physical equivalent of the program/service?
- Privacy and security
  - Recordings
  - Data exhaust
  - Zoombombings

First we have to talk about the recent change from the year that kept on giving – 2020. The rapid shift from physical to virtual work left libraries scrambling to set up secure work and programming environments. Working from home presents several privacy and security issues ranging from staff using personal computers for work to the security of the home network. Many libraries increased their use of third party applications in the switch to remote work, which then leads to the possibility of more patron data being collected by these third parties.

This reliance of third party applications is also a privacy issue with shifting physical patron services and programs to virtual. One particular concern are web conferencing platforms such as Zoom, Webex, and Adobe Connect. These platforms have the ability to collect patron data that otherwise would not have been collected if the patron attended the physical equivalent of the program or service. This leads into the concern that libraries might not be able to guarantee the same level of privacy for online programs as the physical program. These platforms and other services are also subject to disruptions by trolls and serial harassers through zoombombing, causing harm to patrons and library workers alike. The ability to record patron interactions is of additional privacy concern. Again, third parties may not have the same level of legal and ethical requirements as libraries.



Discussion – Your experiences with shifting to virtual



Library Surveillance of Patrons

Library Security

- Security incident databases
- Shift logs
- Security cameras
- Body cameras on security staff/police

Vendor Tracking

- Web analytics
- Data from library vs data from patron
- Behavioral tracking
  - Cross-site
  - Social media
- Marketing and data disclosure/reselling

Library Data Analytics and Marketing

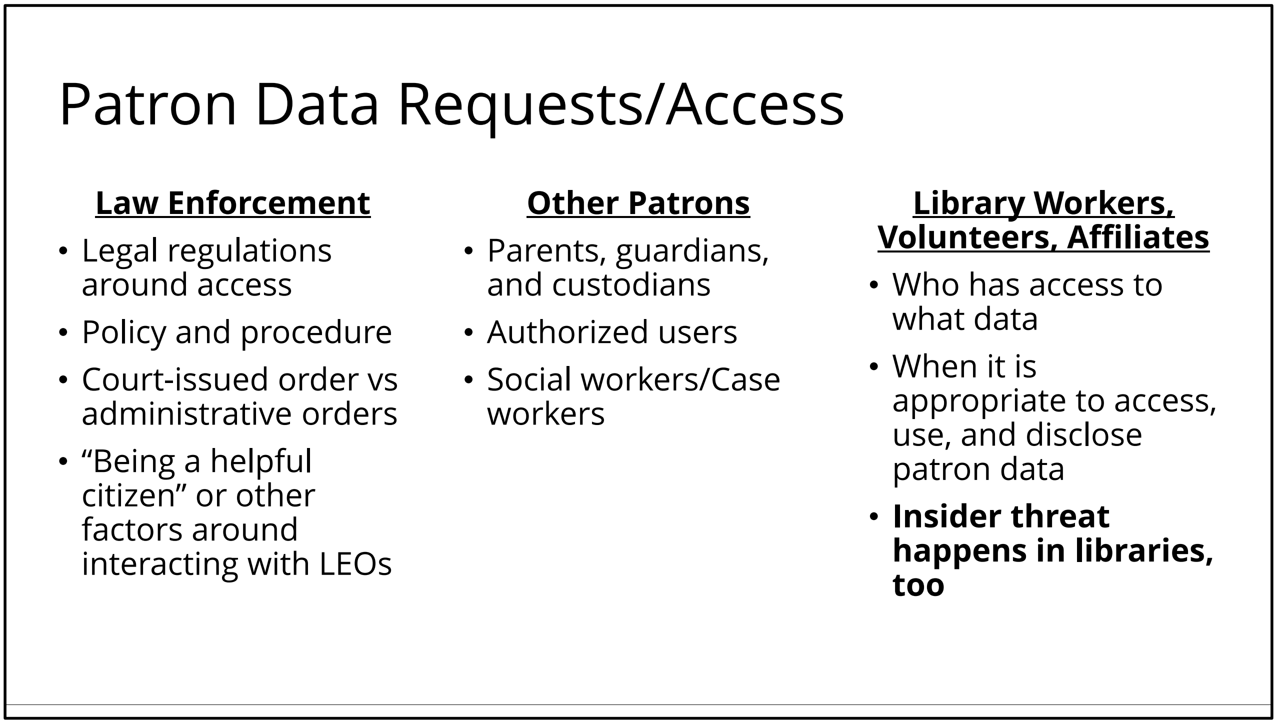
- Patron profile of use of library
- Use of external data sets to create segments
- Primary use of data vs secondary use
- Patron expectations

Surveilling patrons is another area of concern when it comes to patron data privacy. Under 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 surveillance.

Library security is not new, but the technology used has rapidly changed in recent years. 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. Another gray area is the use of security cameras in libraries. Security camera recordings may or may not be considered a patron use record, depending on the placement of the camera and what the camera captures in terms of library use by patrons.

Vendors have an extensive toolbox to collect patron data, including web analytic software, cookies, and web beacons. Vendors also collect patron data directly from the library – for example, asking the library to upload patron data to set up an email subscription management system. The library could send just the bare minimum needed to set up the system – in this case, the email address and if the patron opted in or out of library emails. However, vendors ask above and beyond what is needed, and several library comply with that ask without asking questions. Vendors also have the ability to collect patron data through cross-site tracking as well as incorporating other third party applications for additional functionality, such as logging into the vendor resource using a social media account. On top of all of this, vendors use this data for marketing and reselling purposes, in which many patrons might not be aware of in the first place.

However, vendors are not the only ones to use patron data for analysis and marketing. An increasing number of libraries are creating profiles of patrons through market segmentation and data analytic tools. Often these tools incorporate external data sets that contain data about the patron that the patron did not directly give to the library, such as income and education level. Patrons didn't expect this data to be collected by the library in the first place, so this also comes to the question of how libraries explain to patrons about how the library uses patron data. In practice, it is considerably difficult to use patron data for marketing or analysis while operating within privacy policies and standards, patron expectations, and data and professional ethics.



Patron Data Requests/Access

Law Enforcement

- Legal regulations around access
- Policy and procedure
- Court-issued order vs administrative orders
- “Being a helpful citizen” or other factors around interacting with LEOs

Other Patrons

- Parents, guardians, and custodians
- Authorized users
- Social workers/Case workers

Library Workers, Volunteers, Affiliates

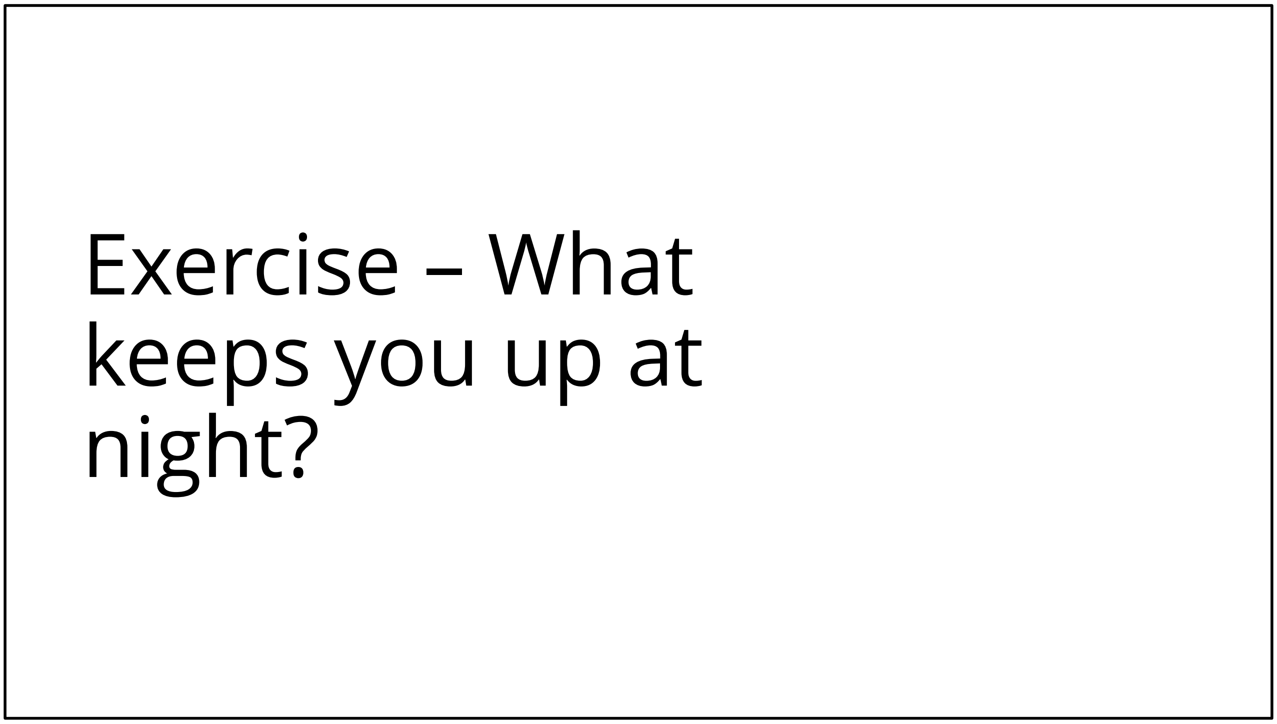
- Who has access to what data
- When it is appropriate to access, use, and disclose patron data
- **Insider threat happens in libraries, too**

The issue of who has access to patron data continues to be a key issue around patron privacy.

Law enforcement usually is one of the first things to come to mind when we talk about patron data requests. Section 6267 protects patron use records from disclosure except for a few cases, such as a court-issued order. The policies and procedures around law enforcement access can vary depending on the request, from an officer asking who is in the building to a request to seize physical hardware for an investigation. ALA has extensive guidelines regarding building policies and procedures around law enforcement requests to create local policy and procedure, including only giving the data explicitly requested in the court-issued order, and not volunteering additional information beyond what the order requested. However, many still cooperate with law enforcement without following policy and procedure for a variety of reasons, including undertraining staff and the expectation to be a helpful citizen.

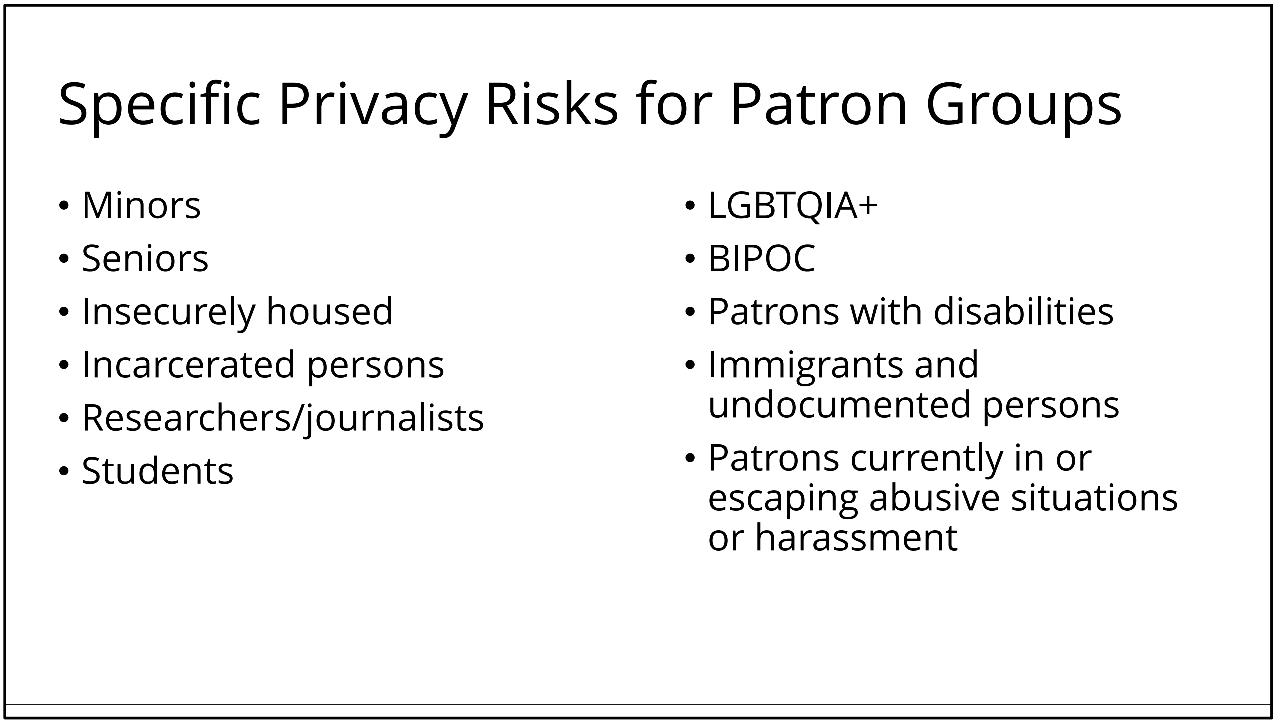
We also have other patrons asking for another patron’s data. Who should have access to another patron’s data? How much data should they have access to? The amount of access and the type of data that can be accessed depends on who the other patron is and why they need access to that patron’s data. The level of access a parent might have for their minor child’s account will differ from the level of access the same parent might have when they want to be authorized to pick up their partner’s holds at the library.

Library workers, volunteers, and affiliates (such as board members) all have the potential to access patron data. Good information security practices around data access can help mitigate some risk around accidental unauthorized access, including giving the least amount of access to the data needed for one to perform their duties and specifying when it’s appropriate to access certain types of patron data. Nonetheless we still have to plan for the possibility of a staff member or volunteer accessing patron data with malicious intent, such as stalking and harassment. This is a concern that keeps me up at night as a library privacy professional.



Exercise – What keeps you up at night?

Follow-up question - which one have you experienced a privacy breach with while working in a library? What were the consequences?



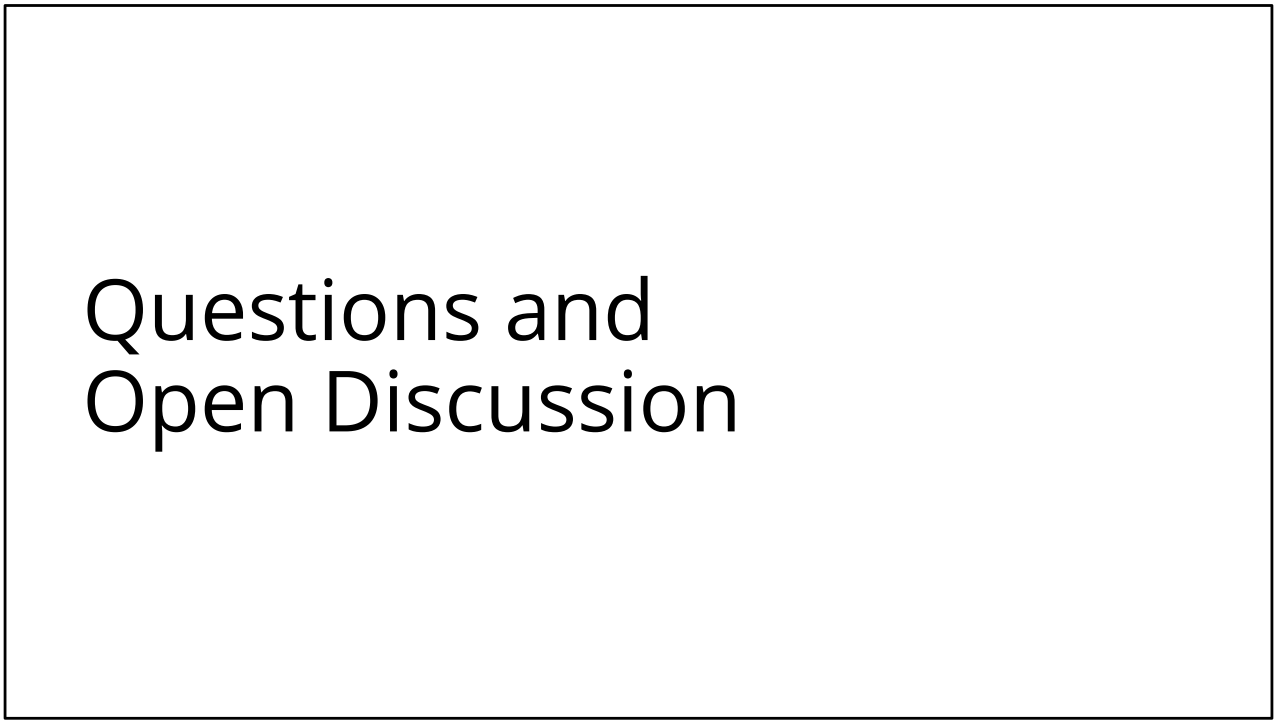
Specific Privacy Risks for Patron Groups

- Minors
- Seniors
- Insecurely housed
- Incarcerated persons
- Researchers/journalists
- Students
- LGBTQIA+
- BIPOC
- Patrons with disabilities
- Immigrants and undocumented persons
- Patrons currently in or escaping abusive situations or harassment

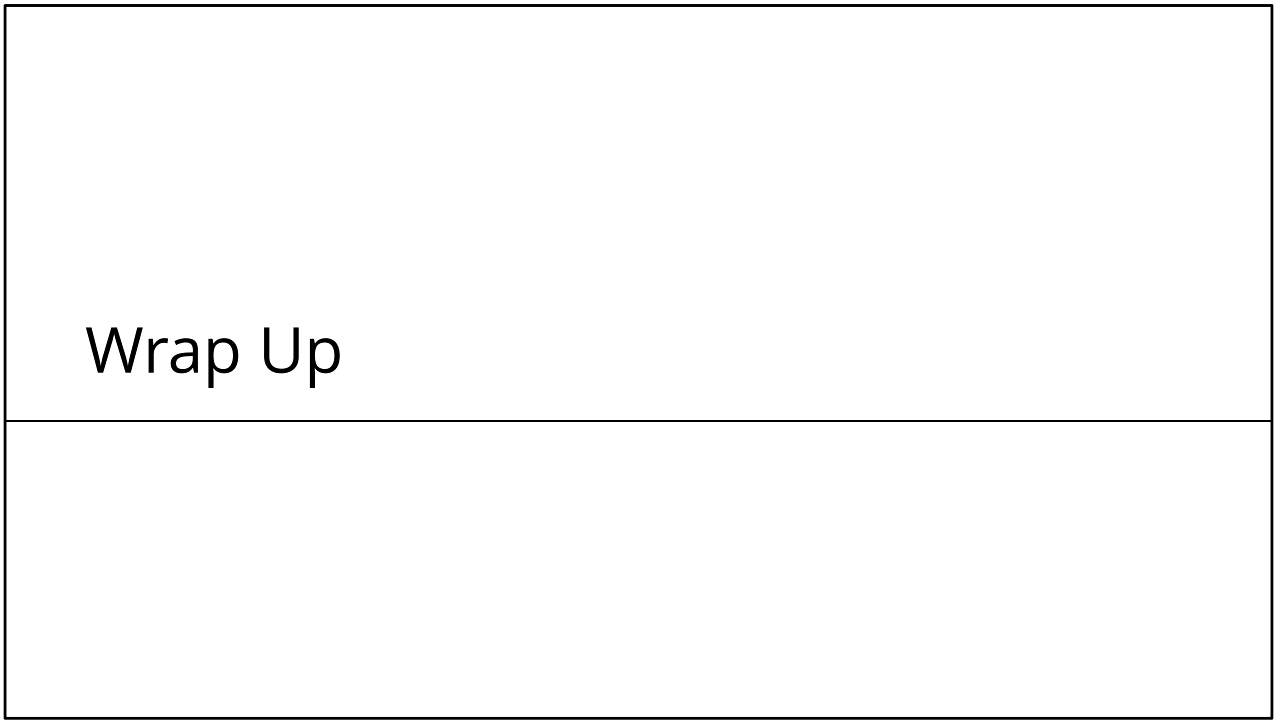
Certain patron groups are at higher risk for harm if their privacy is compromised. One example is the address of a patron being improperly released to another patron, without the staff person knowing that the requesting patron is stalking the other patron. Another example is a patron being harmed by their family or community for researching specific topics around sexuality or religion.

Libraries also put these patron groups at risk while trying to serve these same communities. Patrons requesting ADA accommodations are put at risk when staff overcollect medical information about the patron and store the medical information in unsecured locations. I knew someone who, after receiving a file from a public records request for library staff communications, found the medical records of a patron in a staff email included in that file. In another instance, a library offering English language classes for their EOL patrons was collecting information on if the patrons planned to take the citizenship exam, which is a proxy for determining if the patron was a US citizen.

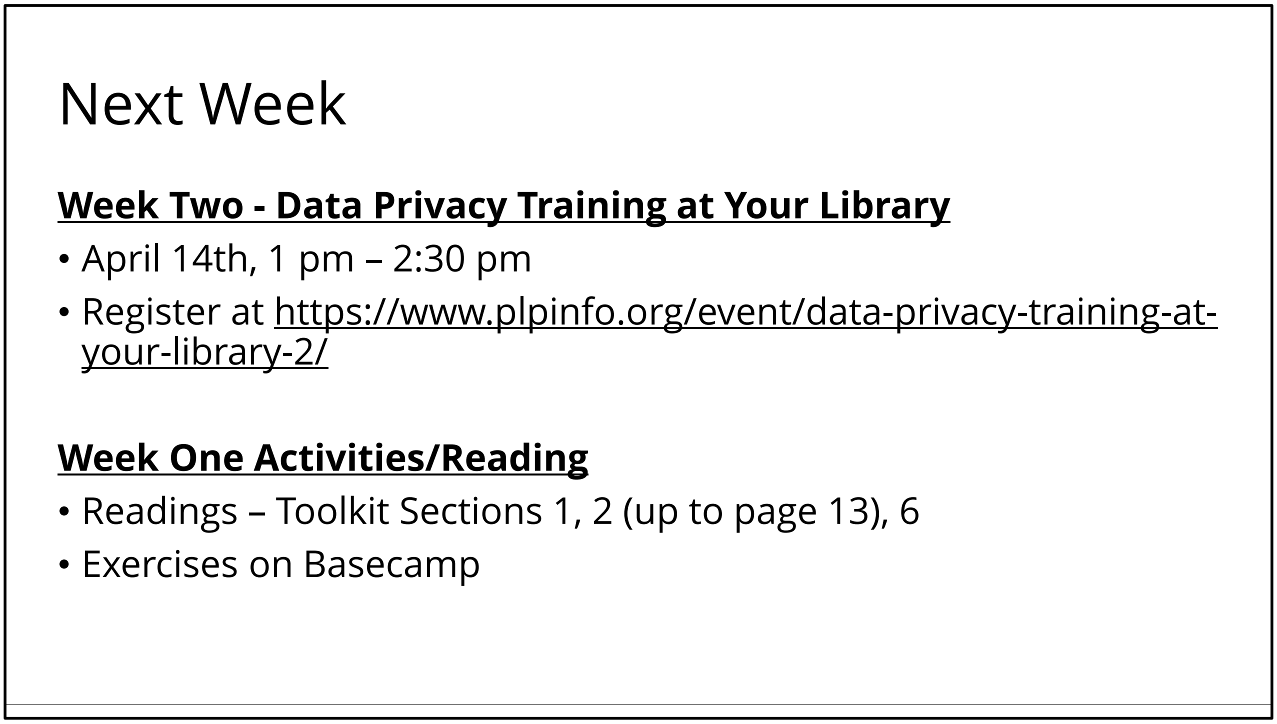
As we go through the series, it is wise to think about how your privacy trainings and practices can help mitigate these additional risks for these patron groups. Adopting a compliance mindset helps meet minimum standards and regulations, but a patron-centric approach to data privacy can cover the wide gaps that a compliance-only approach leaves in any privacy program.



Questions and Open Discussion



Wrap Up



Next Week

Week Two - Data Privacy Training at Your Library

- April 14th, 1 pm – 2:30 pm
- Register at https://www.plpinfo.org/event/data-privacy-training-at-your-library-2/

Week One Activities/Reading

- Readings – Toolkit Sections 1, 2 (up to page 13), 6
- Exercises on Basecamp

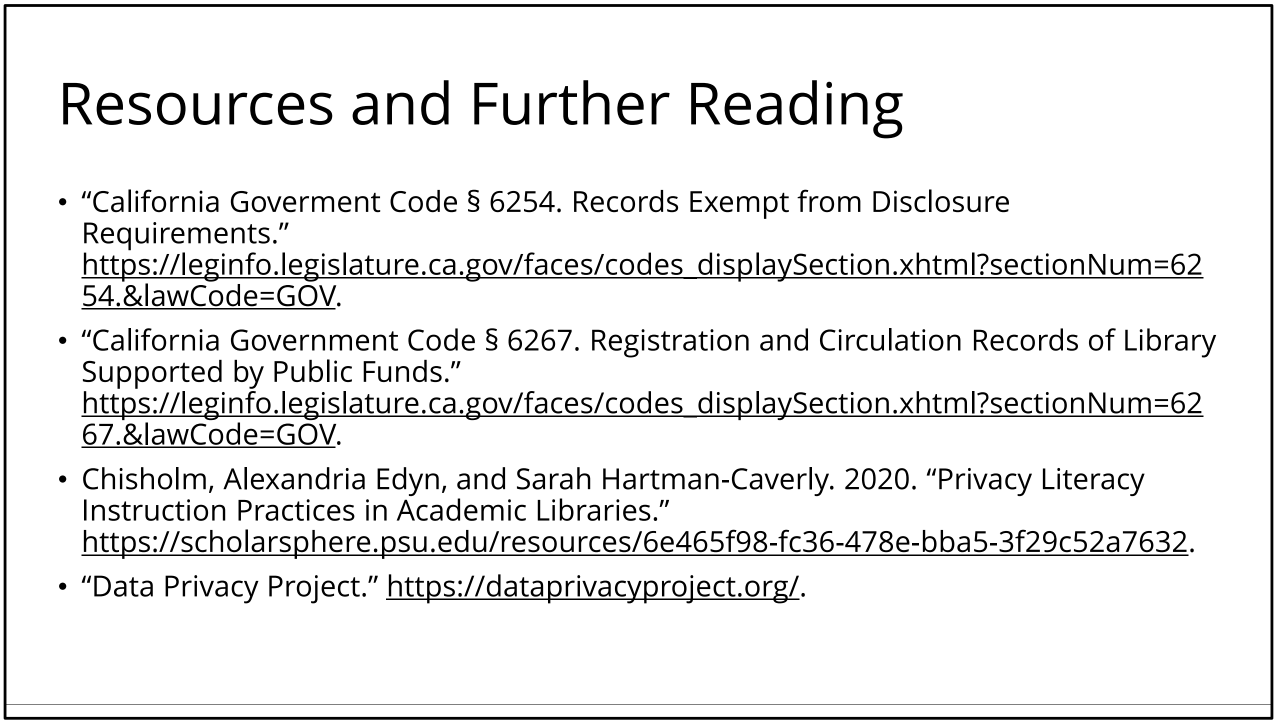
Thank you

:-)

LDH Consulting Services

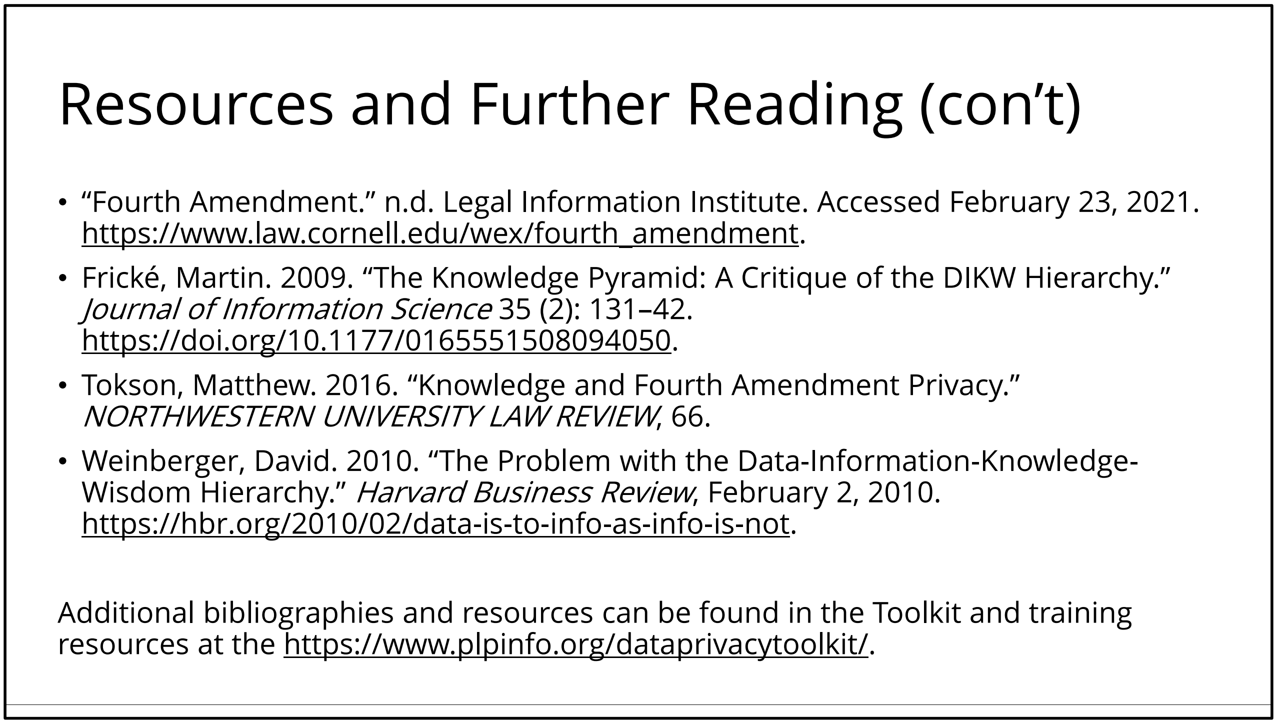
Becky Yoose
Library Data Privacy Consultant
LDH Consulting Services

Email:
becky@ldhconsultingservices.com



Resources and Further Reading

- “California Goverment 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.
- Chisholm, Alexandria Edyn, and Sarah Hartman-Caverly. 2020. “Privacy Literacy Instruction Practices in Academic Libraries.” https://scholarsphere.psu.edu/resources/6e465f98-fc36-478e-bba5-3f29c52a7632.
- “Data Privacy Project.” https://dataprivacyproject.org/.



Resources and Further Reading (con’t)

- “Fourth Amendment.” n.d. Legal Information Institute. Accessed February 23, 2021. https://www.law.cornell.edu/wex/fourth_amendment.
- Frické, Martin. 2009. “The Knowledge Pyramid: A Critique of the DIKW Hierarchy.” *Journal of Information Science* 35 (2): 131–42. https://doi.org/10.1177/0165551508094050.
- Tokson, Matthew. 2016. “Knowledge and Fourth Amendment Privacy.” *NORTHWESTERN UNIVERSITY LAW REVIEW*, 66.
- Weinberger, David. 2010. “The Problem with the Data-Information-Knowledge-Wisdom Hierarchy.” *Harvard Business Review*, February 2, 2010. https://hbr.org/2010/02/data-is-to-info-as-info-is-not.

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