Building and Fostering a Culture of Privacy

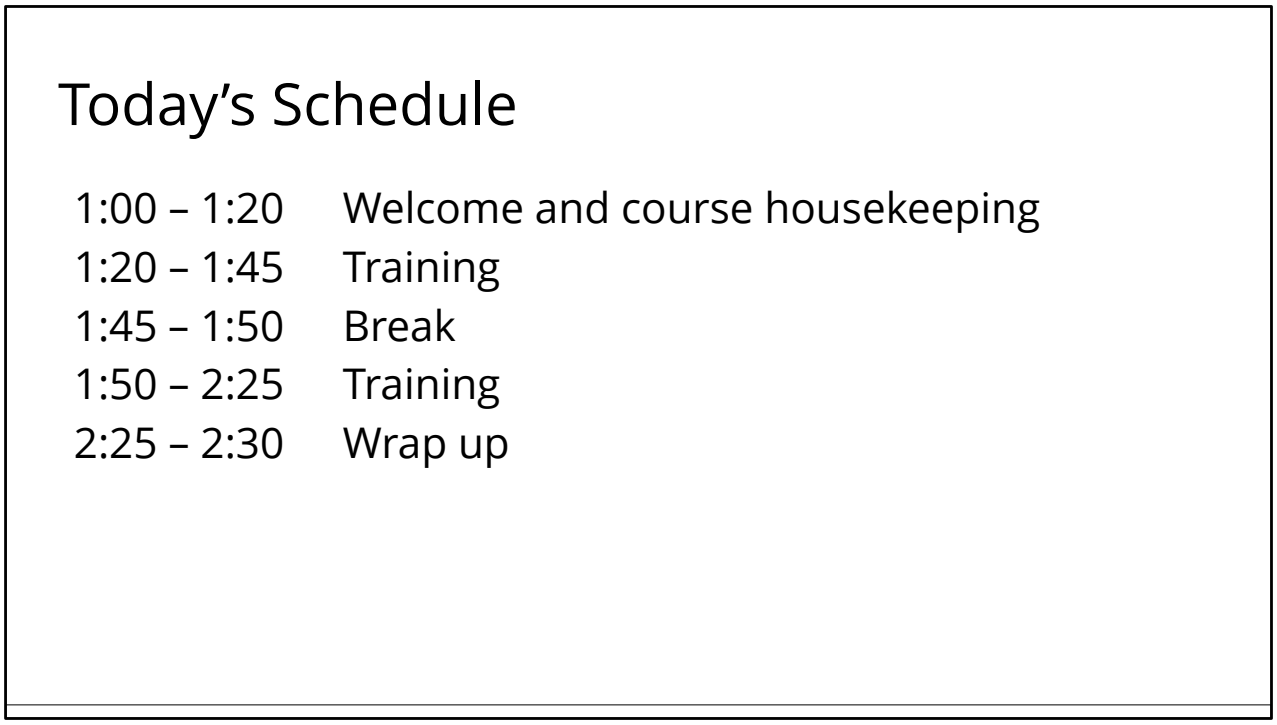
Becky Yoose
Library Data Privacy Consultant, LDH Consulting Services
Data Privacy Best Practices Training for Libraries
April 2021
Week 4

Pacific Library Partnership

Welcome back to the final week of the series! Today we talk about centering privacy in library operations and culture.

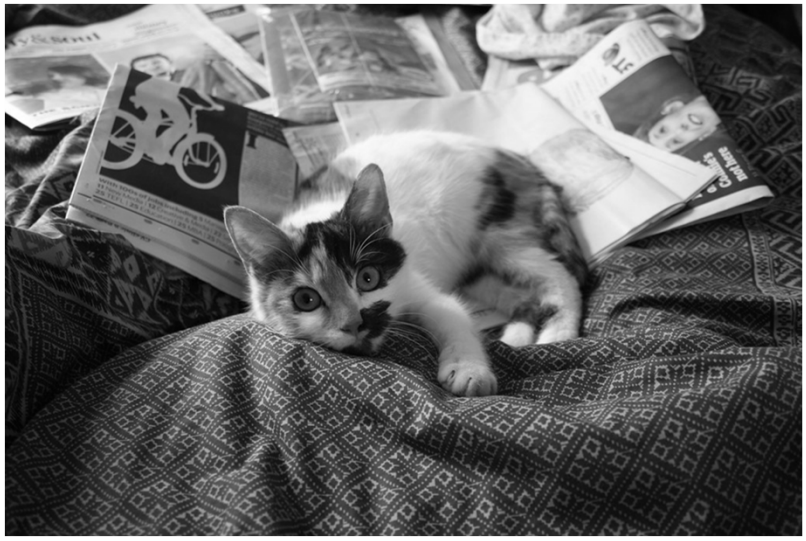
This project was supported in whole or in part by the U.S. Institute of Museum and Library Services under the provisions of the Library Services and Technology Act, administered in California by the State Librarian. The opinions expressed herein do not necessarily reflect the position or policy of the 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.

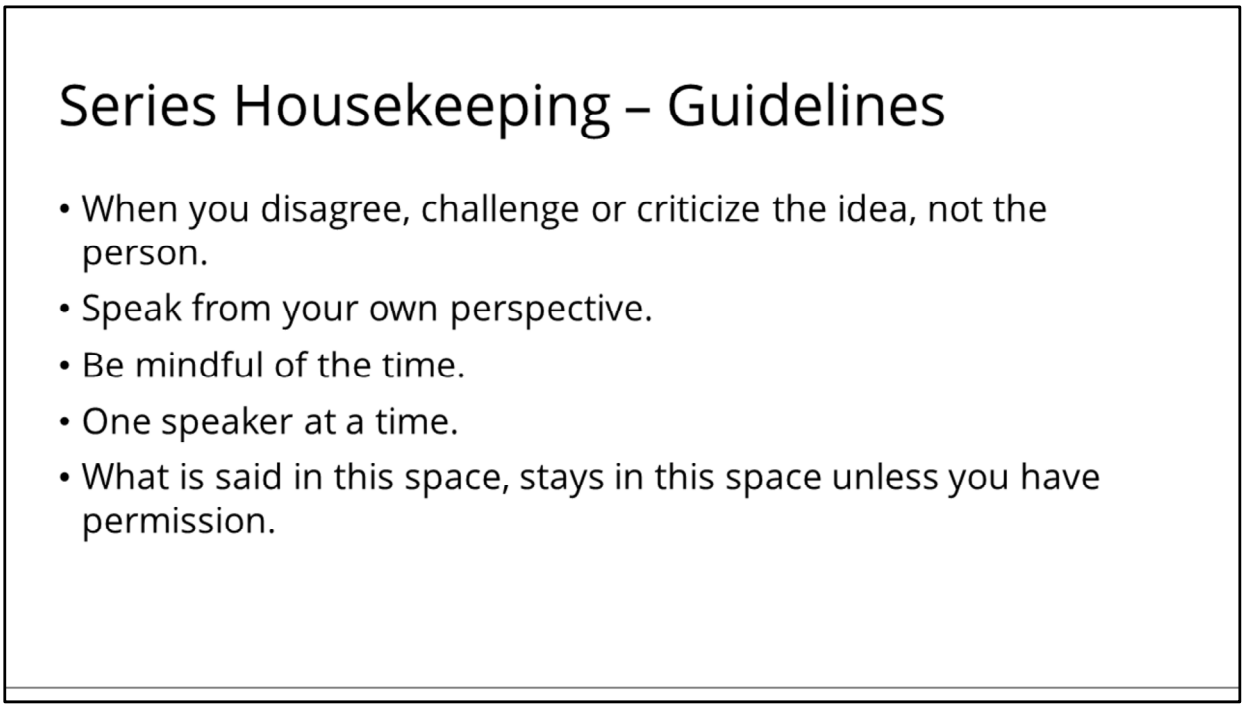


We'll try to keep close to the schedule posted in the slide. There will be some time for Q&A at the end of the session, so if any questions pop up during the presentation, you can enter them in the chat box so we can answer them then.

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.

Fill in the blank – The greatest challenge in implementing a culture of privacy at my library is_____.

If you're here today, you most likely know that patron privacy is important. However, your library might not prioritize patron privacy. Take a moment to complete the sentence: "The greatest challenge in implementing a culture of privacy at my library is…"

1. Privacy and Organizational Culture

Today's session starts with the elephant in the room, organizational culture.

Privacy programs fail because…

- Lack of funding, including dedicated/adjusted budget lines
- Lack of resources
- Lack of dedicated staff time
- Lower priority over other parts of library operations
- Lack of buy-in by any part of the library (staff, volunteers, admin, board, etc.)
- Lack of support by decision makers and administration
- **Unaddressed organizational culture issues often compound the above factors of failure**

In Week two, we talked about the needs for building and sustaining a privacy training program. Organizational privacy programs share some of the same needs and fail points. Lack of funding, lack of dedicated staff time, and lack of resources all play a part. There's also the danger of getting bumped down the priority list due to lack of support from decision makers or administrators or overall lack of buy-in in the library. These are not unsolvable problems, but they do take time to work through. So why then does it seem that they are insurmountable?

This is because when you add unaddressed organizational culture issues on top of these problems, you come up against a seemingly unmovable wall.

Organizational Culture is Hard to Change

It's hard to change organizational culture. This has been well researched and documented. This is why change management exists. When you try to address cultural issues in an organization, more often than not you hit a wall. Literally. Most likely we all have horror stories about a time when someone tried to get something going in the organization, only to… well. And we all probably tried more than once, hitting the wall just the same.

[Image description - A young adult running up to and throwing themselves against an exterior stone building wall.]
[Image source - https://gph.is/XKp9zS]

Organizational Culture and Coping

Common organizational culture issues

- Communication
- Tension between people, departments, offices, etc.
- Office politics
- Unchecked power dynamics
  - Territory struggles
  - Race/ethnicity, gender identity, sexuality, disability, etc.

Coping strategies

- Spend political or professional capital wisely
- No matter what you do, you will fail sometimes
- **You alone will not solve your organization's dysfunctions**

Identifying organizational issues will not guarantee that your privacy program attempts will succeed. Nevertheless, you will at least be able to anticipate these issues when they arise and how to cope in an organization that resists change.

On the left side of the screen are some of the common issues you might come across in any organization. Communication is a perennial organizational issue, whither it be lack of established communication lines, convoluted communication practices, or other issues. Interpersonal relationships also factor into organizational issues, such as fraught relationships between departments or offices, or between key individuals in the organization. Another way interpersonal relationships affect organizational culture is through your garden variety office politics.

Power dynamics can also be a source of organizational issues. We sometimes find these dynamics in territorial struggles within an organization over "who gets what" in terms of budget, resources, and staff. Reshuffling of resources or duties from one person or department to another might be construed as an attack or loss of ground in the organization. It can also be construed as favoring one person or department over another, depending on the redistribution. A person's identity – their race, ethnicity, gender identity, sexuality, disability, and so on – can also shape the power dynamic between individuals and the organization. This power dynamic can be exploited through further marginalization of

minoritized populations in the organization.

With all that said, there are a few ways you can cope with these issues. The first is figuring out how much political or professional capital you have and how much you can realistically spend in addressing these issues. You can fight every fight, but you will find that approach will easily eat up time, resources, and motivation. Strategically choosing what issues to address can boost the chances of success.

Sometimes, though, no matter what you do you end up failing. Sometimes things fail because of factors out of your and the audience's control. The best you can do is to regroup and determine your next actions.

There is the temptation to fix your workplace's dysfunctions. You might be successful in creating small spaces that function better than the overall organization. Nonetheless, the reality is that organizations have a life of their own, and are resistant to long-term changes. Focus on what you realistically have the power to influence in your organization. This might mean focusing on small acts of privacy at your organization. Remember, though, that sometimes the smallest acts can lead to the biggest changes.

Stakeholders and Creating Buy-in

- Library administrators
- Legal counsel
- Library board
- Library workers
- Parent organization/institution
- Patrons
- Community partners

- What are the motivators and concerns?
- What can they relate to in terms of interests, beliefs, experiences, etc.?

Because privacy affects everyone at the library, the following stakeholders on the slide should have some part in creating the privacy program.

Some of the stakeholders play a direct part – your legal counsel need to ensure that your policy doesn't miss any regulations, and your administrators or board have the final say of what policies is approved. However, it would be amiss if we only focus on the administration and legal staff. Library workers on all levels are key in creating and sustaining organizational-wide change and practices. If your library is part of a bigger organization, they too also have a part to play since they in part shape the library organizational practices. You also need to go beyond the organization and bring in patrons and community partners who represent specific patron groups. Again, if your privacy program doesn't center the patron, you will most likely leave many patrons open to privacy risk.

So how do we work with stakeholders in a way that it doesn't seem like we're just checking the box in a list? We observe, we ask questions, and most importantly we listen. What are their motivators and concerns? Some people are mainly motivated by making sure that their organization is in legal compliance. This might be a good thing if you're trying to get your work to follow a particular regulation, but not so great if that regulation is not very effective in protecting patron privacy. Others are motivated by various types of pride, be it in the workplace, personal, or civic pride of being a good community member or library

professional. Organizational culture and politics can be either a motivator or concern. A collaborative culture among colleagues can play in your favor, while an organization that has turf wars between departments, and even within departments, can be a concern for a person who is afraid that they might lose power or status if they work with others.

The second question is figuring out what they can relate to in terms of interests, beliefs, and experiences. For example, a number of technology workers come from backgrounds that do not have strong professional ethics codes, so they might not get why librarianship's ethics codes are so important. Another factor is that some folks can only relate with others with the same backgrounds, beliefs, and experiences. Or, to be blunt, they just relate to people who look like and act like them. This one is tricky to work with, and you might have to hedge your bets if the person is not willing to step out of their comfort zone. It's wise to anticipate this and find other ways that this person can relate – research or reports can be persuasive for some who trust current research practices.

[Image description - Five people of color sit side by side at a rectangular meeting table.]
[Image source - https://www.flickr.com/photos/wocintechchat/22344392878/ (CC BY 2.0)]

Identifying Needs and Gaps

- Surveys (within reason)
- Department/team/group meeting listening sessions
- Informal meetings (coffee/hallway chats)
- Community conversations/listening sessions
- Privacy and security audits
- Data inventories and risk assessments

The last two questions can provide useful information about the privacy needs and gaps at your library. There are several ways you can gather this information from people, from group listening sessions to informal or impromptu chats over coffee. You can also use surveys, but you need to be mindful about survey fatigue. Like not everything has to be a meeting, not everything has to be a survey.

In conjunction to working with stakeholders, you will need to do some work with audits, inventories, and risk assessments to identify potential needs and gaps that might not be covered in your conversations. These do not have to be comprehensive in covering every application, and process, but you might find it worthwhile to audit or assess a process or system if that process or system keeps coming up in your conversations with stakeholders. Having that audit or assessment report can help refine your buy-in pitch to those stakeholders who are affected or work with those processes and systems.

[Image description: A Black woman raises her hand among other adults attending a town hall meeting.]
[Image source: https://phil.cdc.gov/Details.aspx?pid=11617 (Public Domain)]

Achieving Buy-in – Strategies

- Come to the table and make a place for yourself
- Have vocal allies in the organization that will support your ideas
- Come with a story that aligns to their motivations and concerns
- Come with a realistic actionable plan or outline
- Strive for positive-sum outcomes

All that listening we did in the past two slides needs to be reflected in the way you approach privacy buy-in in the organization. Building a privacy program proposal that combines your ideas with motivations and concerns of stakeholders will help increase the chance of buy-in, but ultimately achieving buy-in takes a good amount of time and resources, and unfortunately, lots and lots of meetings. (I'm sorry).

Sometimes we get lucky and we have a spot on the table in organizational discussions and decisions. If that's not the case for you, find that spot on the table in such a way that people won't feel like you just barged in. If you have strong relationships with others at the table, they can negotiate a place for you to lessen that chance of others at the table feeling threatened in terms of possible changes to organizational power balances.

This might go without saying, but never underestimate having vocal allies in the organization. The more organizational influence and power they have, the better; however, don't discount the influence strong allies in the front lines have in an organization. A bottom up approach can be as effective as having a strong privacy advocate in administration. Allies are also very good people to get feedback and perspective on proposals and plans.

Another big factor that affects buy-in is if you bring an actionable plan that is within the

means of your organization. This again needs to reflect the motivations and concerns of your audience. An example of this is available resources, though you also want to make the argument to shift responsibilities if you are proposing staff time and changes in duties for existing staff so that they actually have the dedicated time to work on the projects you're proposing.

Finally, a good general rule to keep in mind while influencing all the people is to aim for positive-sum outcomes. Reframing your conversations as a "how can this plan benefit everyone" talk can help you determine which areas in the plan are most important to prioritize, and which areas are the most important to your audience in terms of realizing and inclusion.

[Image description: An adult woman sits at a long oval conference table with several stuff animals sitting in their own chairs around the table.]
[Image source: https://www.flickr.com/photos/80403443@N00/69821764 (CC BY 2.0)]

Group Therapy, Session #1	Think of a time when you took part of a project or effort to implement a system-wide change in the organization. • What were you trying to change? • Were you successful in implementing the change? • What contributed to the success/failure?

Think of a time when you took part of a project or effort to implement a system-wide change in the organization. What were you trying to change? Were you successful in implementing the change? What contributed to the success/failure?

2. Building Privacy into Organizational Culture – Frameworks and Standards

Creating buy-in is one part in creating a culture of privacy. Another part is building that privacy structure into the organization. This section will get into several privacy frameworks and standards used by other libraries and in other industries to help you get started down that path.

Privacy Frameworks – Privacy by Design

1. Proactive not reactive; preventive not remedial
2. Privacy as the default setting
3. Privacy embedded into design
4. Full functionality – positive-sum, not zero-sum
5. End-to-end security – full lifecycle protection
6. Visibility and transparency – keep it open
7. Respect for user privacy – keep it user-centric

When we talk about privacy frameworks, one of the first ones to come to many people's minds is Privacy by Design. Developed in the mid '90s, Privacy by Design's goal is to imbed privacy all parts of a process or project. This is, in part, to avoid having privacy tacked on at the end of a process or project, where it's much harder to implement privacy effectively. You might have encountered this with other things with other projects. For example, it's harder to make a website accessible when you only test for accessibility at the very end of the website design project instead of designing with accessibility in mind throughout the project.

Privacy by Design has seven founding principles. Some of these principles are self explanatory – for example, making sure that you are ahead of the curve when it comes to addressing potential privacy issues, or having a privacy component in planning, implementation, and maintenance of a product or service. These could take the form of having a check embedded into any process to align products and services to privacy policies. Other principles require organizations to approach privacy in a inclusive manner. In particular, I want to call out numbers 4, 6, and 7, in this respect. Transparency and a user-first approach will require adjustments to communication and decision making processes. Number 4 requires a shift in the framing of any privacy discussion. We tend to think of privacy as a compromise, or that we can either have privacy or we have data needed to keep our libraries in business. By reframing privacy from a "this OR that" to a "this AND

that”, you can then focus privacy work on how to accommodate the needs and concerns of everyone involved without priming them for a figurative fight to get their needs met by the product or service.

Overall, Privacy by Design does a fairly good job in conveying a comprehensive organization-wide approach to privacy, when combined with other frameworks and standards to shore up the gaps.

[Image description - A door lock switch turned to the arrow printed with the word "PRIVACY" on the label.]
[Image source – https://www.flickr.com/photos/pong/2404940312/ (CC BY 2.0)]

Privacy Frameworks – Privacy by Default

- Moves from embedded privacy considerations in operations (PbD) to making privacy the default in operations
- Set highest level of privacy settings and risk mitigations as starting point (auto-protect)
- Shifts some of the burden of protecting patron privacy from the patron to the library

Even though privacy by default is a principle in Privacy by Design, regulations and industry trends have moved this principle to its own framework. This takes the embedded approach of Privacy by Design – asking for privacy to be considered at each stage of a process or operation – and makes it explicit in requiring the organization to choose the highest level of privacy settings or mitigation strategies in any process or system. For patron-facing systems, patrons could change these settings to the level of privacy that they are comfortable with, but all accounts would start with the highest level of privacy possible in the system.

One reason why there's a push toward privacy by default is due to the near impossibility of end users to navigate privacy settings and policies as they are presented to the user. In the privacy profession there is an increasing number of people who believe that notice and consent are not effective in protecting user privacy. Notice and consent center around informing the patron and the patron having the ultimate responsibility for their privacy. However, when research shows that users are already overwhelmed, is it ethical for organizations to solely rely on notice and consent to manage user privacy? Good design and communication practices can help, but the library's privacy practices should reflect the reality that patrons are overwhelmed and might not have the resources to effectively protect their privacy at the library.

[Image description: Visual notes from GSMA's Director of Privacy Pat Walsche's talk at Mobile Mondays Brussels on world-wide privacy recommendations. Major points from the notes:

- Privacy done right & building trust is a business opportunity.
- Privacy is a place to be alone, without fear of observation.
- Users do care: 92% is concerned about their personal data, 81% is doing efforts to safeguard their data, and 76% is selected whom they share data with.
- There's a patchwork of data laws, and (luckily) many local privacy guidelines initiatives are started, however, there is hardly any coordination world-wide.
- The cookie laws have actually undermined privacy, as they got people used to saying "Yes", regardless if the degree of 'invasiveness' of data being collected
- There's also definitely issues on OS level.
- Privacy (done right) is a huge business opportunity.
- All stakeholders in the mobile ecosystem have the responsibility to help build trust. Stop scaring customers away.]

[Image Source: https://www.flickr.com/photos/vintagedept/10692059443/ (CC BY 2.0)]

Privacy Frameworks – Data Ethics

"Data ethics are the norms of behavior that promote appropriate judgments and accountability when collecting, managing, or using data… ethical decision making is best achieved by taking a holistic approach and widening the context to weigh the greater implications of data use."

~ Federal Data Strategy; Data Ethics Framework

Common data ethics principles

- Transparency
- Accountability
- Professional and industry ethics and best practices
- Equity
- Centering and empowering the individual behind the data

This leads us into the world of data ethics. In the privacy world we talk about different types of breaches, such as security and data breaches. However, you can be in compliance with legal regulations and still run the risk of an ethics breach. Ethics breaches are the failure to handle data consistent with organizational or professional values.

Data ethics can help you minimize the risk of an ethics breach. While discussions around the ethical use of data are not new, there has been some efforts in recent years to come up with a framework or set of principles for guiding organizations in their use of data. One example is the Data Ethics Framework as part of the US Federal Government's Federal Data Strategy. In this framework, data ethics is defined as the behavioral norms that inform decisions and actions around data collection, management, and use. Data ethics is further defined as a holistic approach in determining the impact of data decisions.

There are a few common threads in the FDS framework and other data ethics frameworks from the UK and in the private sectors, including transparency and accountability in decisions around data use, as well as following industry ethics and best practices such as data minimization. Data ethics frameworks share the charge to put context around data management to focus on how this management impacts the individuals behind the data, including different impacts on different populations. Data ethics places the onus on the organization to manage data to minimize risks to individuals. While traditional approaches

to data privacy, such as notice and consent, places this onus squarely on the individual, data ethics takes into the account the reality that organizations are in a position to take advantage of their users and their data in ways that can harm users.

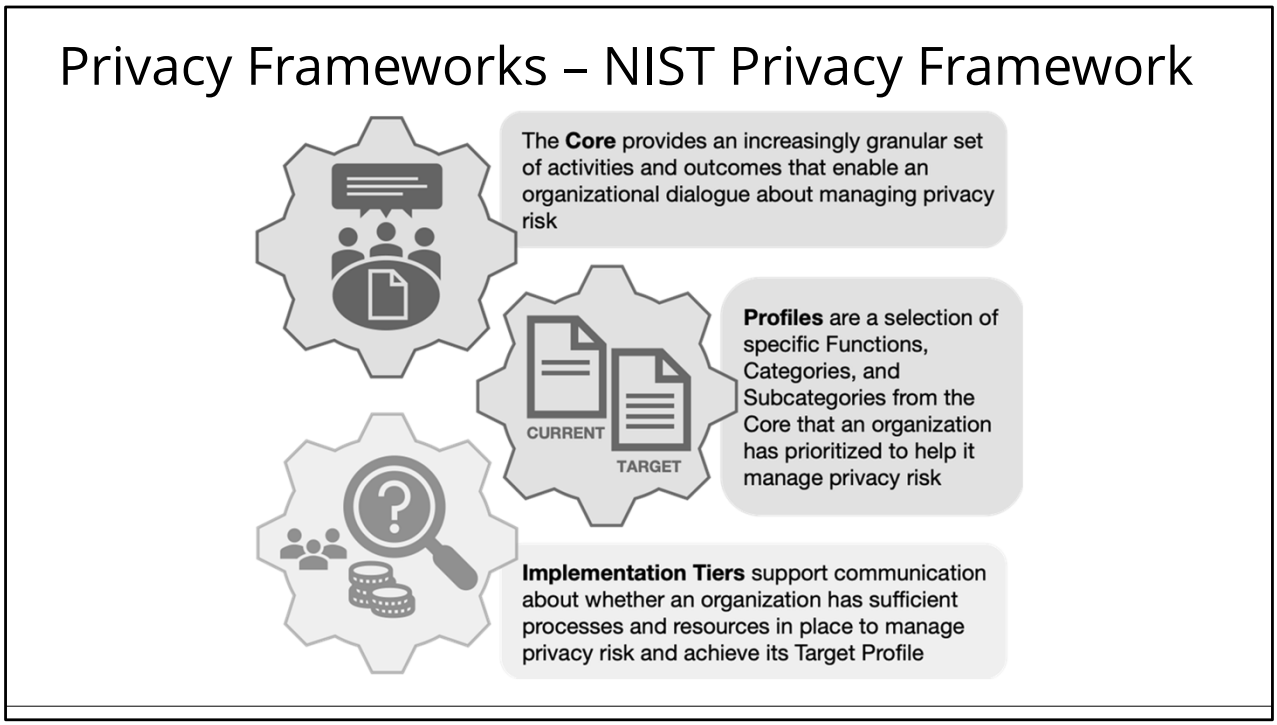
“Ethics is knowing the difference between what you have the right to do and what is right to do.”

- Potter Stewart, US Supreme Court Chief Justice

In short, Potter Steward’s definition of ethics sums up the ethos behind many data ethics frameworks.

Data Ethics Litmus Test	How do patrons react when they learn about the library's data practices?

The accountability and transparency of data ethics frameworks can be used to create a quick litmus test. How do patrons react when they learn about the library's data practices? If your patron's reaction to your data practices is "you did *what* with my data?", you have a possible data ethics breach. There should be no major surprises for differences between the expectations created through privacy notices and other communications from the library to patrons about data management, and what the library actually does with patron data.



Data ethics, Privacy by Design and by Default are fairly high level frameworks. Some organizations require more structure or guidance in implementing comprehensive privacy practices. Here, I can give you a couple of frameworks and standards that can provide more guidance, depending on the level of detail and structure needed for your organization.

If you are looking for a comprehensive privacy framework that has a wide range, from granular individual activities to broad profiles of current and target privacy practices, the National Institute of Standards and Technology has you covered with their Privacy Framework. The Framework comes in three interdependent parts: the Core, Profiles, and Implementation Tiers. We'll spend the next few slides going into what each part entails.

[Image description
[Image source: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf]

Function	Category	Subcategory
COMMUNICATE-P (CM-P): Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks.	**Communication Policies, Processes, and Procedures (CM.PO-P):** Policies, processes, and procedures are maintained and used to increase transparency of the organization's data processing practices (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) and associated privacy risks.	**CM.PO-P1:** Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks are established and in place.
		CM.PO-P2: Roles and responsibilities (e.g., public relations) for communicating data processing purposes, practices, and associated privacy risks are established.
	Data Processing Awareness (CM.AW-P): Individuals and organizations have reliable knowledge about data processing practices and associated privacy risks, and effective mechanisms are used and maintained to increase predictability consistent with the organization's risk strategy to protect individuals' privacy.	**CM.AW-P1:** Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place.
		CM.AW-P2: Mechanisms for obtaining feedback from individuals (e.g., surveys or focus groups) about data processing and associated privacy risks are established and in place.
		CM.AW-P3: System/product/service design enables data processing visibility.
		CM.AW-P4: Records of data disclosures and sharing are maintained and can be accessed for review or transmission/disclosure.
		CM.AW-P5: Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources) in the data processing ecosystem.
		CM.AW-P6: Data provenance and lineage are maintained and can be accessed for review or transmission/disclosure.
		CM.AW-P7: Impacted individuals and organizations are notified about a privacy breach or event.
		CM.AW-P8: Individuals are provided with mitigation mechanisms (e.g., credit monitoring, consent withdrawal, data alteration or deletion) to address impacts of problematic data actions.

NIST Privacy Framework – Core

The **Core** is the activities and outcomes for protecting privacy in an organization. These are broken down by *Function*, *Category*, and *Subcategory*. For example:

- Communicate-P (the P is there to differentiate from NIST's Cybersecurity Framework) is a *Function* in which the organization is developing and implementing activities and discussions to aid understanding how data is processed as well as the privacy risks associated in that processing.
- A *Category* of the Communicate-P Function is Communication Policies, Processes, and Procedures, which is creating and maintaining policy and procedures around data processing and transparency around privacy risks.
- The *Subcategories* of the Category are what you would expect from building a communications plan: who is doing the communicating, what needs to be communicated and in what format.

It might be tempting to use the Core as a checklist; however, that is not the purpose of the Core. You don't have to go in order of the Core, or complete all subcategories in a category, either. According to the framework, an organization chooses which categories and subcategories best meets their goals in risk management, legal compliance, industry standards and best practices, and the privacy needs of those who are directly impacted by the organization's data processing.

[Image description: A screen capture of the COMMUNICATE-P Function table in the NIST

Privacy Framework Core document, including the Function's category and subcategory entries.]
[Image source: https://www.nist.gov/document/nist-privacy-framework-v10-core-doc]

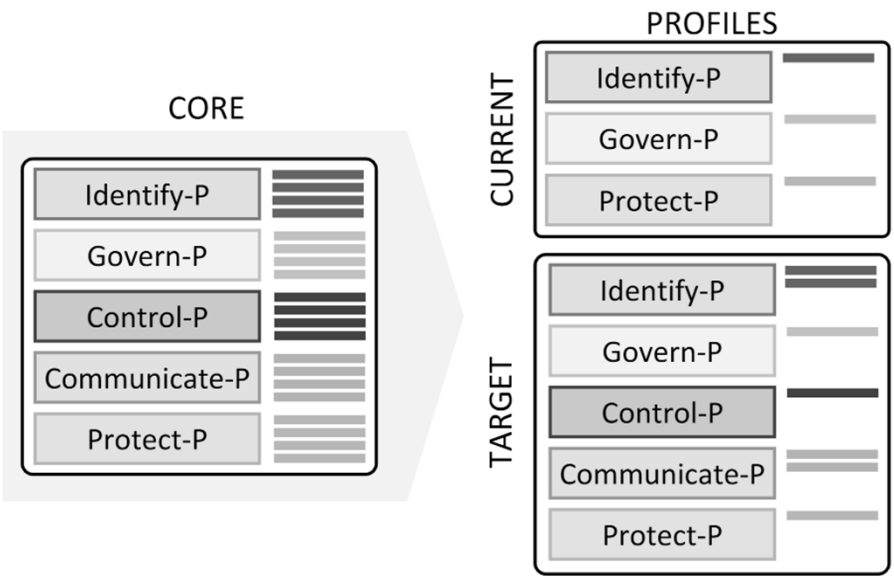


Figure 6: Relationship Between Core and Profiles

The **Profile** plays two roles – it can represent the current privacy practices of an organization, as well as a target set of practices for which the organization can aim for. A *Current Profile* lists the current Functions, Categories, and Subcategories the organization is currently doing to manage privacy risks. The *Target Profile* helps businesses figure out what Functions, Categories, and Subcategories should be in place to best protect privacy and to mitigate privacy risk.

[Image Description – The left column box labeled CORE contains five functions and each function contains four solid bars representing categories. The right column labeled PROFILES has two boxes labeled CURRENT and TARGET, each with an incomplete set of functions and categories.]
[Image source - https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf, Figure 6]

Library Privacy Ethics, Standards, and Guidance

ALA

- Library Bill of Rights
- Privacy: An Interpretation of the Library Bill of Rights
- Code of Ethics
- Policy concerning Confidentiality of Personally Identifiable Information about Library Users
- Library Privacy Guidelines and Checklists
- Video and electronic surveillance technologies guidance
- Law enforcement request guidance

IFLA

- IFLA Statement on Privacy in the Library Environment
- IFLA Code of Ethics for Librarians and other Information Workers

CLA and California State Library

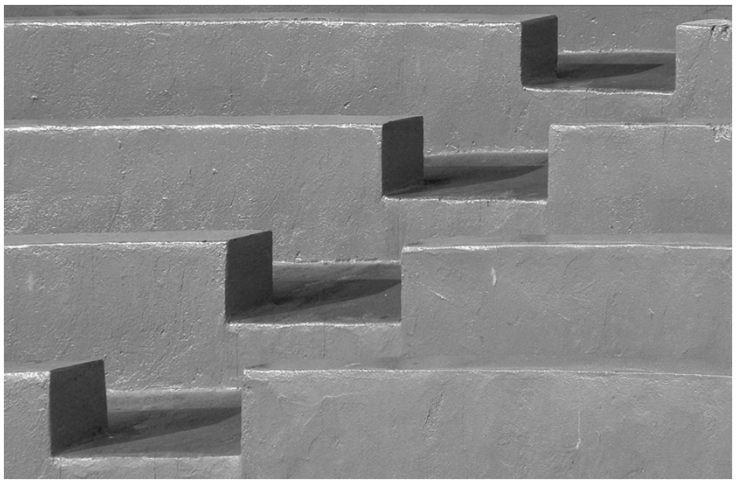
- Statements and recommendations (example – LinkedIn statement by both organizations)

At this point you might be wondering how you would determine what exactly your target profile should be. NIST's Privacy Framework's flexibility can incorporate several library ethics codes, standards, and other policy guidance from organizations. ALA has several resources and policies that you can use to evaluate and prioritize which categories and subcategories to choose for your target profile. On the screen are just a few of the resources and standards that ALA provides the library profession. These guidelines and checklists provide practical information that can be incorporated into determining your current and target profiles, as well as which categories and subcategories you will need to prioritize.

IFLA, CLA, and the California State Library also have resources to help with determining which categories and subcategories to choose for your target profile.

NIST Privacy Framework - Tiers

- Tier 1, Partial
- Tier 2, Risk Informed
- Tier 3, Repeatable
- Tier 4, Adaptive



The ***Implementation Tiers*** are a measurement of how the organization is doing in terms of managing privacy risk. There are four Tiers in total, ranging from minimal to proactive privacy risk management. Organizations can use their Current Profile to determine which Tier describes their current operations. Target Profiles can be developed with the desired Tier in mind. Note that while all organizations can improve their privacy management practices by moving from Tier one to two, it might be that the Target Profile tops out at Tier three. Not all organizations can realistically achieve Tier Four, or in some cases even Tier Three. The most important thing is to focus on achieving the outcomes outlined in the Target Profile.

[Image description: Four rows of tiered turquoise concrete benches with steps cut into each bench.]
[Image source: Photo by Marco Bianchetti on Unsplash, https://unsplash.com/photos/ptaBA0dS1Ek]

Implementing Privacy Frameworks & Programs

A Simplified Method for Establishing or Improving a Privacy Program

Ready: use the Identify-P and Govern-P Functions to get "ready."

Set: "set" an action plan based on the differences between Current and Target Profile(s).

Go: "go" forward with implementing the action plan.

Figure 7: Notional Collaboration and Communication Flows Within an Organization

Implementing a privacy framework for a privacy program can get very involved, very fast. On the slide are two figures from the NIST Privacy Framework that not only applies to the framework, but could also apply to general implementation of any privacy program or framework. The larger figure demonstrating the collaboration and communication flows that should happen when you are working with a framework such as the NIST Privacy framework. The three levels – admin, manager, and operations – all have to work together in assessing risks, determining what the current profile is, and create a target profile to then work toward. All levels have individual responsibilities, but it's clear that without a focus on collaboration and communication, each level can't fully perform their duties.

The smaller callout text box is the "quick and dirty" implementation plan, based on a three stage "ready, set, go" model. Again, this is geared toward the NIST Privacy Framework, but you can use this for other privacy program plans. If you are a project manager, or have delved into project management methods, you might find some similarities between this model and creating a project charter with milestones, goals, stakeholder and project team member identification, and deliverables.

Before you head off into project management mode, you also need to account for what comes after the project. After managing a project, you end up with a product, and that product needs managing as well. This leads into product management, where you manage

how the product is maintained as well as its continued development and eventual sunsetting. Processes are not exempt from needing maintenance – this means resources and staff. Any planning for implementing a framework or privacy program must account for maintenance costs and management.

[Left image description: A light green/blue text callout box titled "A Simplified Method for Establishing or Improving a Privacy Program" listing three actions - Ready, Set, Go - with brief descriptions for each action.]

[Right image description: “Figure 7: Notional Collaboration and Communication Flows Within an Organization.” This figure has three boxes in a row representing three levels: Senior Executives, Business/Process Manager, and Implementation/Operations. Each level has a list of unique responsibilities. Two double ended arrows sandwich the boxes, the top labeled Collaboration and the bottom Communication.]

[Image sources: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf]

Patron-Centered Privacy Design **Good** Design …	**Honors Reality** **Creates Ownership** **Builds Power** ___

We cannot forget that with all our talk about privacy frameworks and standards, it all comes back to the patron. Libraries protect patron privacy because the patron has the right to privacy at the library. Our privacy practices, therefore, should center on the patron.

We covered a lot of information in this four week series and it's very easy to get lost in the details. Ultimately, when we start building a privacy program in a library, we're designing a system to carry out a particular function or need. How we design this system affects its effectiveness and impact. Taking a framework by George Aye from Greater Good Studio about Good Design, good design achieves three goals, all of which can be applied to designing a library privacy program:

Honoring reality – how can the library meet the demonstrated needs of the organization while honoring the different expectations of privacy among library patrons?

Creating ownership – how can the library give patrons a sense of ownership over their data and privacy?

Building power – what should the library do in order to provide agency to patrons surrounding data collection and sharing? What data rights must be present to allow patrons control over the library's use of their data? How can patrons have a voice in the

development, implementation, and review processes for privacy practices at the library, including those most at risk? How will you ensure that the process will not just be a “mark the checkbox” but instead an intentional act to include and honor those voices in the process?

Answering these questions can help you adapt those frameworks to center the patron in your privacy program.

https://www.tamarackcommunity.ca/hubfs/Events/Multi-Day%20Events/2019%20CCF%20Vancouver/Resource%20Uploads/2019%20CCF%20Keynote%20-%20George%20Aye.pdf?hsLang=en

Group Therapy, Session #2	Using the scenario for Session #1, how could the frameworks and standards discussed in this section aid in your change efforts?

Using the scenario for Session #1, how could the frameworks and standards discussed in this section aid in your change efforts?

3. Keeping Up

We’re almost to the end! The rate of change in privacy law, standards, and practices shows no signs of slowing down. Library privacy practices are going the same route with increased reliance on data as well as changes in technology, vendor relations, and services. With all this rapid change, it’s even more important to find ways to keep current on issues, trends, and developments.

Professional Development and Resources

- Work groups
- Online communities and interest groups
- Internal documentation and resource sharing
- Training (online, in person, conferences)
- Sharing examples and stories from news, posts, other colleagues
- ALA's Choose Privacy Every Day
- Library Freedom Project
- IMLS grant funded projects
- IAPP
- Electronic Frontier Foundation
- Future of Privacy Forum

There are several strategies you can use to keep up with professional development. If you're the type of person who needs a group of people for motivation and accountability, you can create interest or study groups at work that center around privacy in general or specific privacy concerns or tools. These groups can be used to discuss current privacy news and updates or to train or practice a particular skillset (such as data security). This approach allows you to start building a community of practice in your organization, where privacy advocates and those interested in learning more about privacy can come together to share knowledge and discuss how the organization's approach to privacy is working or can be improved. You'll also find several online communities and interest groups outside the library that focus on many facets of privacy, from privacy law to issues of equity in privacy.

Groups are not the only way to build a community of practice in your organization. Sometimes having an internal site page dedicated to sharing of resources and documentation about library privacy can help you and others keep on top of professional development. Training is another option, be it online training, classes, or conference events. The sharing of resources can also include sharing examples and stories of "how things were done right" as well as "let's try to avoid having this happen to us" from news and colleagues from other libraries.

On the right side of the screen is a starter list of resources for information about library privacy or privacy in general. ALA's Choose Privacy Every Day provides privacy news and posts about current privacy topics in libraries, as well as serves as a clearinghouse for privacy resources created by the organization. The Library Freedom Project's Library Freedom Institute is a great program to learn more about how to advocate for privacy not only in libraries, but also in your communities. On their website you can find resources that you can use for patron programming as well as guiding library privacy practices and vendor management. IMLS has funded several library privacy focused projects in recent years, and they also will or have already produced resources for libraries to use for specific privacy topics, such as web tracking and learning analytics.

As for privacy in general, the International Association of Privacy Professionals, IAPP, is a fantastic resource to keep up on privacy legislation news and issues. The Electronic Frontier Foundation, EFF, provides both news and resources to help you keep up with issues and trends around privacy and technology. Finally, it's worthwhile to keep track of research and publications from the Future of Privacy Forum around privacy issues, trends, and practices.

Discussion – Sharing is Caring!

What other resources do you use to keep current on privacy issues? Strategies? Other privacy information?

Where do we go from here?

We've reached the end of the workshop series. By now you're probably wondering where to start given the number of topics we've covered in the series, from privacy training to implementing privacy frameworks.

- Training
- Policy and Procedure
- Programming

(Need more help? Head to the Action Plan exercise on Basecamp!)

Echoing the slide about coping strategies when trying to change organizational culture, focus on what you realistically have the power to influence in your organization. Given that you are attending a “train-the-trainer” series, privacy training is a natural place to start, as well as incorporating privacy topics into existing digital literacy and skills patron programming. Policy and procedure reviews or creation is another starting point, particularly if you can get administration buy-in for a comprehensive review.

These are three places where you can have an impact in the way that your library approaches patron privacy. You might have more influence and resources to do more, and that’s great! If you’re limited on resources or influence, building relationships might get you both buy-in from key people in the organization as well as resources, be it sharing between departments or through shifts in capital budget spending lines. Being strategic in how you introduce a cultural change in an organization can increase the chances of that change sticking as well as conserving resources and time to continue the momentum that you are building with these successful changes.

[Image description: a pile of colorful skeins of yarn and roving on a white carpet.]
[Image source: https://www.flickr.com/photos/lacuna007/4551436590/ (CC BY SA 2.0)]

Questions and Open Discussion

Thank you

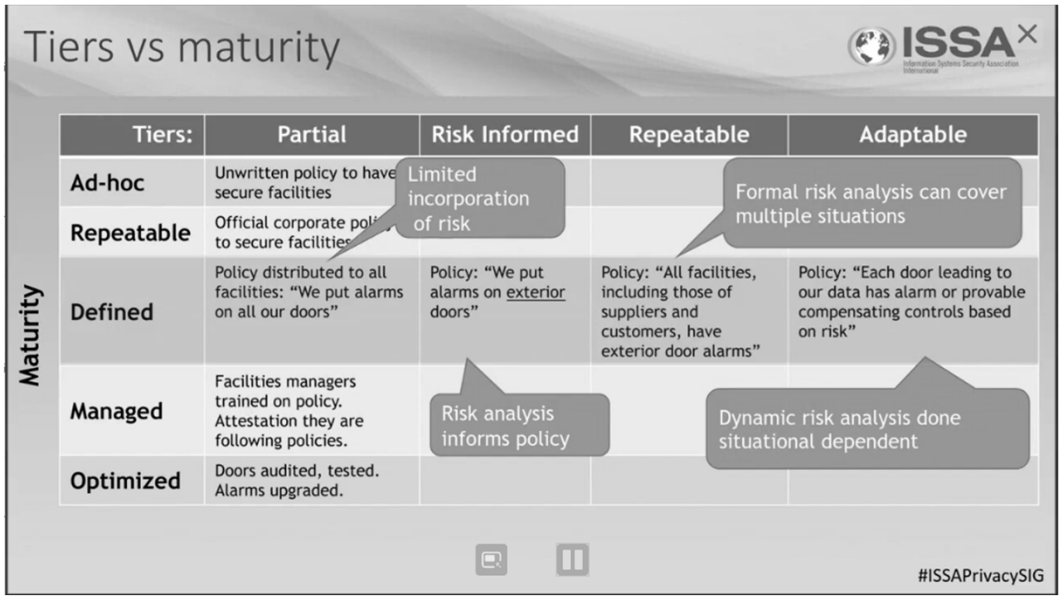
:-)

LDH Consulting Services

Becky Yoose
Library Data Privacy Consultant
LDH Consulting Services

Email:
becky@ldhconsultingservices.com

Bonus Slide! Implementation Tiers in NIST Privacy Framework



Bonus slide!

This is a screenshot from a presentation about the NIST Privacy Framework demonstrating how the Implementation Tiers are different from maturity levels. Even when there are gaps in privacy practices, there can still be optimized privacy practices under Tier One (Partial).

The Core and Implementation Tiers are not prescribed checklists, but instead guidance for organizations to develop a target profile that reduces privacy risks in an organization. In addition the highest realistic tier for an organization might not be Tier Four due to resources and the types of risks the organization wants to address.

Image source: Giordan, Scott and R. Jason Cronk. "ISO 27701 versus NIST Privacy Framework." March 16, 2021. https://www.brighttalk.com/webcast/16125/465975/iso-27701-versus-nist-privacy-framework.

Resources and Further Reading

- ALA. “Choose Privacy Every Day.” https://chooseprivacyeveryday.org/.
- Alboum, Jonathan. 2019. “Why We Need Data Ethics.” ITProPortal. https://www.itproportal.com/features/why-we-need-data-ethics/.
- Alt-Greene, Francine. 2021. “Project Management for Libraries: Project Scope and Charter.” https://minitex.umn.edu/events/webinar/2021-01/project-management-libraries-project-scope-and-charter.
- Blair, Tess. 2019. “What Is Privacy by Design and by Default?” https://www.morganlewis.com/pubs/2019/03/the-edata-guide-to-gdpr-what-is-privacy-by-design-and-by-default.
- “Change Management.” *Wikipedia*. https://en.wikipedia.org/w/index.php?title=Change_management.

Resources and Further Reading

- “Data Ethics Framework.” 2020. Government Digital Service. https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework-2020.
- “———.” 2020. Federal Data Strategy. https://resources.data.gov/assets/documents/fds-data-ethics-framework.pdf.
- Electronic Frontier Foundation. https://www.eff.org/.
- Future of Privacy Forum. https://fpf.org/.
- International Association of Privacy Professionals. https://iapp.org/.

Resources and Further Reading

- NIST. 2013. “Cybersecurity Framework.” NIST. https://www.nist.gov/cyberframework.
- ———. 2020. “Getting Started - NIST Privacy Framework.” NIST. https://www.nist.gov/privacy-framework/new-framework/getting-started.
- ———. 2020. “Privacy Framework.” NIST. https://www.nist.gov/privacy-framework/privacy-framework.
- Sally, David. 2020. *One Step Ahead: Mastering the Art and Science of Negotiation*. New York: St. Martin’s Press.
  - This book is focused on negotiations and can be very useful in vendor negotiations; however, the advice found in this book can apply to talking points and communication strategies for creating buy-in with stakeholders and target audiences.

Resources and Further Reading

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