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

This project was supported in whole or in part by the U.S. Institute of Museum and Library Services under the provisions of the Library Services and Technology Act, administered in California by the State Librarian. The opinions expressed herein do not necessarily reflect the position or policy of the U.S. Institute of Museum and Library Services or the California State Library, and no official endorsement by the U.S. Institute of Museum and Library Services or the California State Library should be inferred.

Today's Schedule

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

Last Week Recap

Series Housekeeping – Guidelines

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

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

1. Privacy and 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**

Organizational Culture is Hard to Change

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**

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.?

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

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

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?

2. Building Privacy into Organizational Culture – Frameworks and Standards

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

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

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

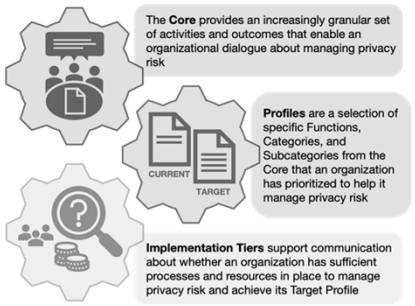
"Ethics is knowing the difference between what you have the right to do and what is right to do."

- Potter Stewart, US Supreme Court Chief Justice

Data Ethics Litmus Test

How do patrons react when they learn about the library's data practices?

Privacy Frameworks – NIST Privacy Framework



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

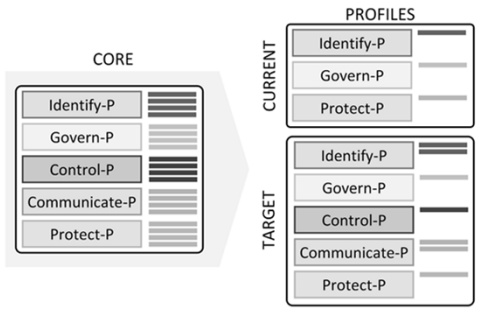


Figure 6: Relationship Between Core and Profiles

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

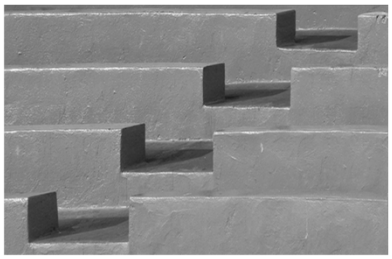
- IFLA Statement on Privacy in the Library Environment
- IFLA Code of Ethics for Librarians and other Information Workers

CLA and California State Library

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

NIST Privacy Framework - Tiers

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



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

Patron-Centered Privacy Design

Good Design …

Honors Reality

Creates Ownership

Builds Power

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?

3. Keeping Up

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

Discussion – Sharing is Caring!

Where do we go from here?

- Training
- Policy and Procedure
- Programming

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

Questions and Open Discussion

Thank you

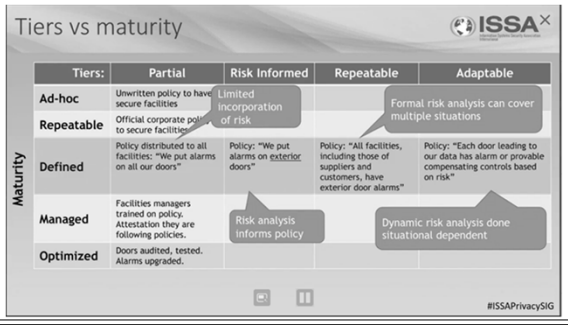
:-)

LDH Consulting Services

Becky Yoose
Library Data Privacy Consultant
LDH Consulting Services

Email:
becky@ldhconsultingservices.com

Bonus Slide! Implementation Tiers in NIST Privacy Framework



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/.