Operationalizing Library Privacy: Policies, Procedures, and Practice

Training Two of the PLP Data Privacy Best Practices Training for Libraries Project

February 2020

Pacific Library Partnership

INSTITUTE of Museum and Library SERVICES

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.

This document does not constitute legal advice, and is for informational purposes only. Please consult an attorney or other legal counsel for legal advice.

Cover Page Photo Credit - Privacy by Nick Youngson CC BY-SA 3.0 ImageCreator

Handbook developed by Becky Yoose, LDH Consulting Services
becky@ldhconsultingservices.com

Table of Contents

Acronyms

ALA	American Library Association
BYOD	Bring Your Own Device
CCPA	California Consumer Privacy Act
CLA	California Library Association
COPPA	Children’s Online Privacy Protection Act
Data FOMO	Data Fear Of Missing Out
FERPA	Family Educational Rights and Privacy Act
FIPPs or FIPs	Fair Information Practice Principles or Fair Information Practices
GDPR	General Data Protection Regulation
IANAL	I Am Not A Lawyer (always a good acronym to have in your back pocket!)
IFLA	International Federation of Library Associations and Institutions
NIST	National Institute of Standards and Technology
PbD	Privacy by Design
PII	Personally Identifiable Information
OECD	Organisation for Economic Co-operation and Development

Workshop Exercises

Exercise - Policy, procedure, practice… and PB&J

A twist on an old exercise! No knowledge or experience in libraries required. Appetite optional.

Your group founder has tasked your group to come up with a policy and procedure for making peanut butter and jelly (PB&J) sandwiches for the public. The "what, when, where, and how" are being left up to your group. The "why" given to you by your founder is that giving sandwiches to the public meets a community need for sandwiches. Your efforts will be funded, so you don't have to worry about budgets!

What should your policy include?

What should your procedures include?

What are some possible factors or issues that might affect your policy and procedures?

Exercise – Privacy Notice Review

Review the privacy notice assigned to your group and discuss the questions below. Assign a note taker and a person to report out to the entire group.

What is one thing that the notice does exceptionally well?

If given the chance to change only one thing about the notice, what would you change?

What assumptions does this notice make regarding the audience of the notice?

Exercise – Privacy Documentation in Action!

Content warnings for one of the scenarios: Physical assault

What should you do? Each group will be given a scenario packet. In your group:

- One person will be the library worker
- One person will be the requester
- The rest will be silent observers during the scenario

Each packet contains the following:

- Procedure and policy documents for the library worker and observers
- Background and scene setting information for all group members

Review the information for your role. Once everyone has reviewed their documents, the library worker and requester have up to five minutes to play out the scenario to the best of their abilities. The silent observers will take notes on the scenario as it happens.

After the five-minute time limit, the group will debrief the scenario from the perspective of their role in the scenario.

Spend some time on each question in the group. Take turns around the group to answer the first question, then moving on to the next question (and the next) once everyone has had a chance to answer the first question:

What happened? What did you notice, what facts or observations stood out?

Why is what happened important or significant?

Now what? What conclusions or lessons from the scenario should be the main takeaways?

Reflection – Design and Reality

Designing a patron-centered privacy program at your organization should:

- **Honor reality** – the privacy program reflects the realities of the patrons who use the library
- **Create ownership** – giving patrons a sense of ownership over their data and privacy at the library
- **Build power** – putting the structures in place in the library for patrons to have agency around their data and privacy at the library, including involvement in decision making processes around privacy policies and procedures

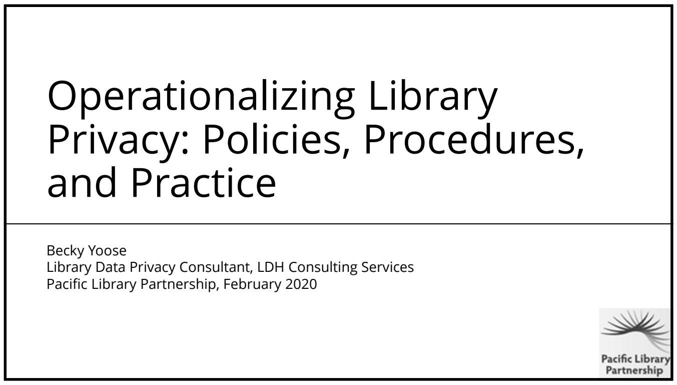
Take a moment to reflect on your own:

What is one way that your current privacy operations honor reality, create ownership, or build power for your patrons?

What is one area in which you could improve privacy operations by adopting a patron-centered privacy program?

What is one major barrier or challenge that might prevent adoption of patron-centered privacy at your library?

How can you address this barrier or challenge?

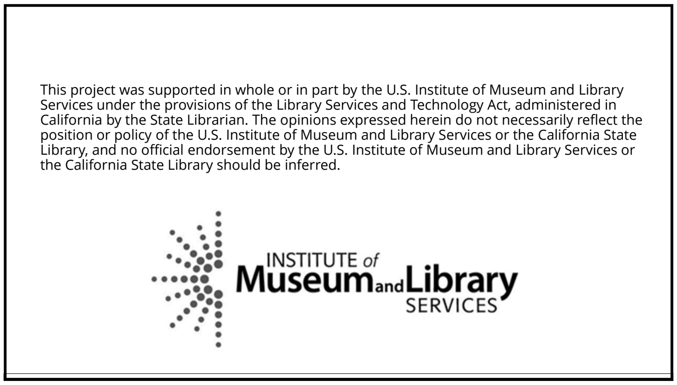


Operationalizing Library Privacy: Policies, Procedures, and Practice

Becky Yoose
Library Data Privacy Consultant, LDH Consulting Services
Pacific Library Partnership, February 2020

Pacific Library Partnership

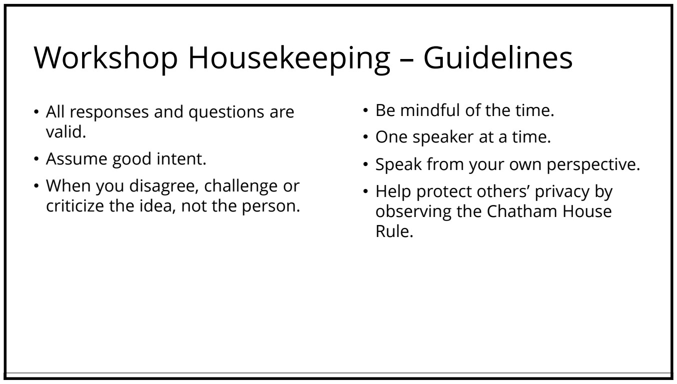
1



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

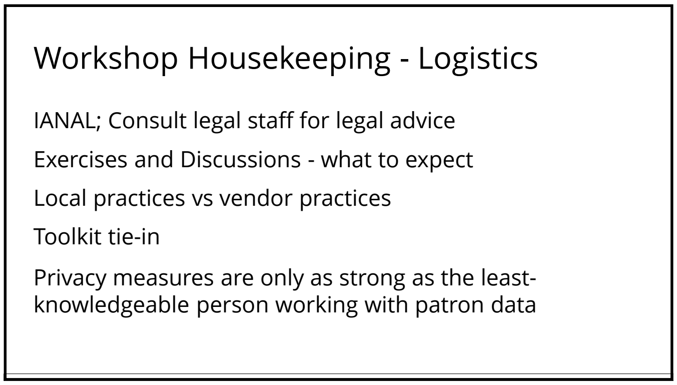
2



Workshop Housekeeping – Guidelines

- All responses and questions are valid.
- Assume good intent.
- When you disagree, challenge or criticize the idea, not the person.
- Be mindful of the time.
- One speaker at a time.
- Speak from your own perspective.
- Help protect others' privacy by observing the Chatham House Rule.

3



Workshop Housekeeping - Logistics

IANAL; Consult legal staff for legal advice

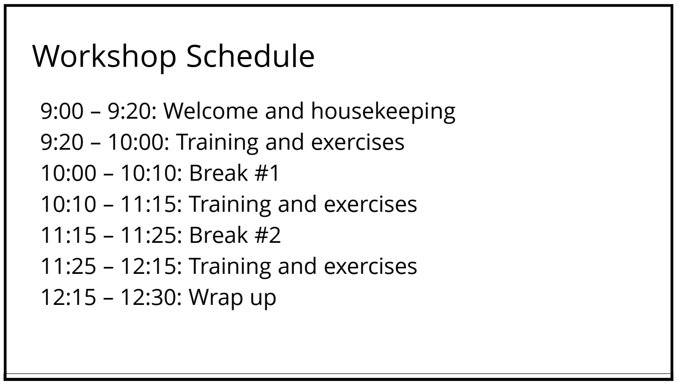
Exercises and Discussions - what to expect

Local practices vs vendor practices

Toolkit tie-in

Privacy measures are only as strong as the least-knowledgeable person working with patron data

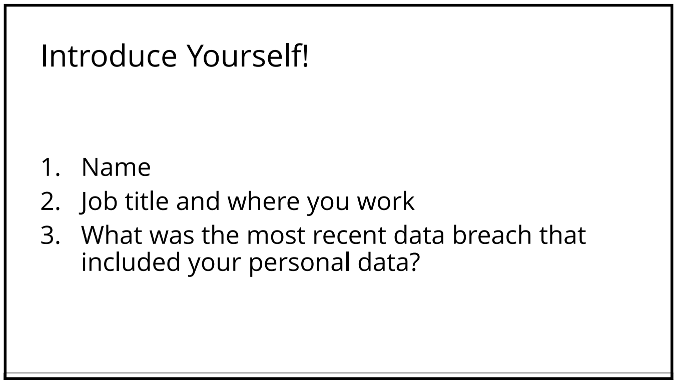
4



Workshop Schedule

9:00 – 9:20: Welcome and housekeeping
9:20 – 10:00: Training and exercises
10:00 – 10:10: Break #1
10:10 – 11:15: Training and exercises
11:15 – 11:25: Break #2
11:25 – 12:15: Training and exercises
12:15 – 12:30: Wrap up

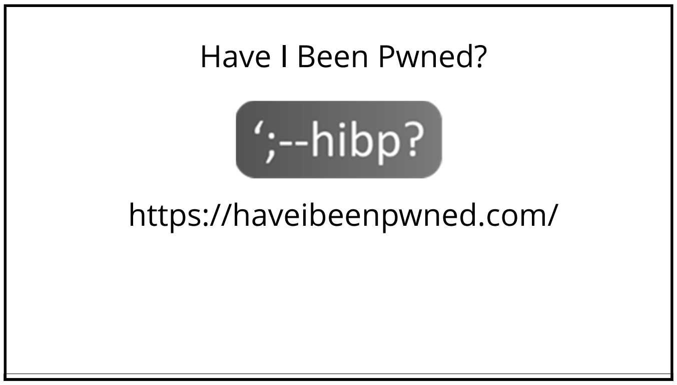
5



Introduce Yourself!

1. Name
2. Job title and where you work
3. What was the most recent data breach that included your personal data?

6

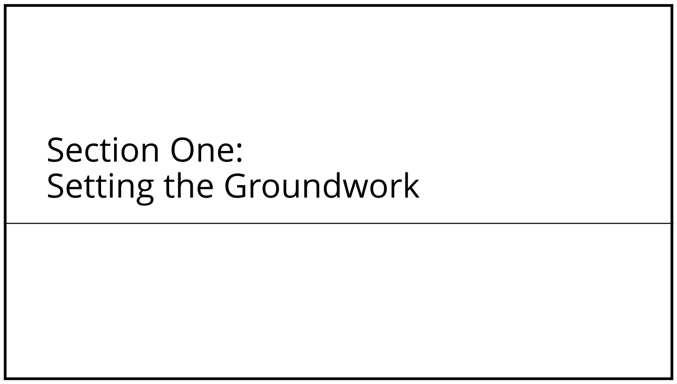


Have I Been Pwned?

';--hibp?

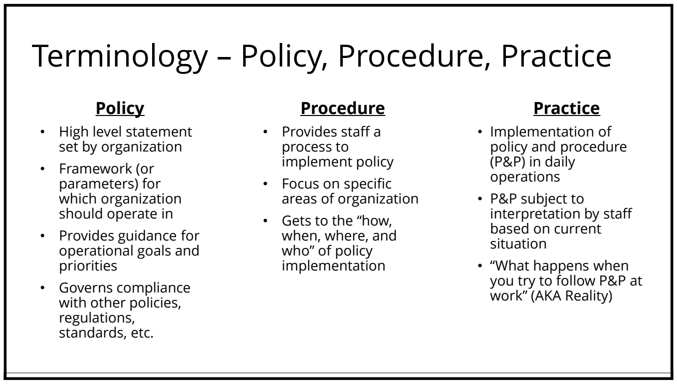
https://haveibeenpwned.com/

7



Section One: Setting the Groundwork

8



Terminology – Policy, Procedure, Practice

Policy

- High level statement set by organization
- Framework (or parameters) for which organization should operate in
- Provides guidance for operational goals and priorities
- Governs compliance with other policies, regulations, standards, etc.

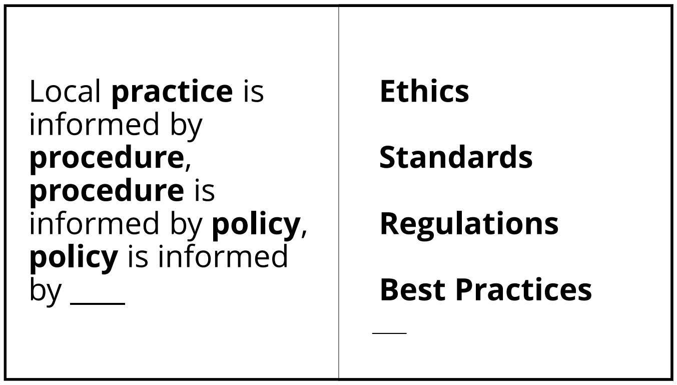
Procedure

- Provides staff a process to implement policy
- Focus on specific areas of organization
- Gets to the "how, when, where, and who" of policy implementation

Practice

- Implementation of policy and procedure (P&P) in daily operations
- P&P subject to interpretation by staff based on current situation
- "What happens when you try to follow P&P at work" (AKA Reality)

9



Local **practice** is informed by **procedure**, **procedure** is informed by **policy**, **policy** is informed by ____

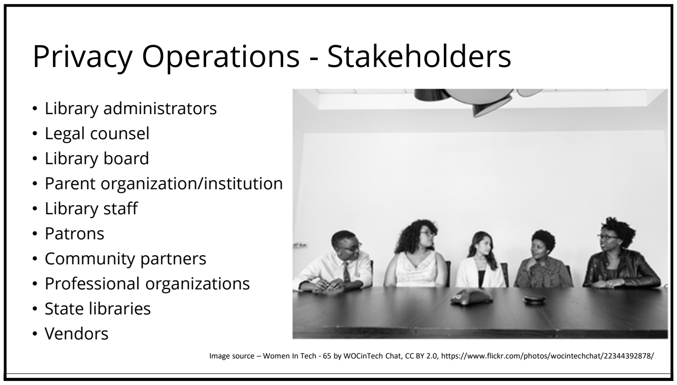
Ethics

Standards

Regulations

Best Practices

10

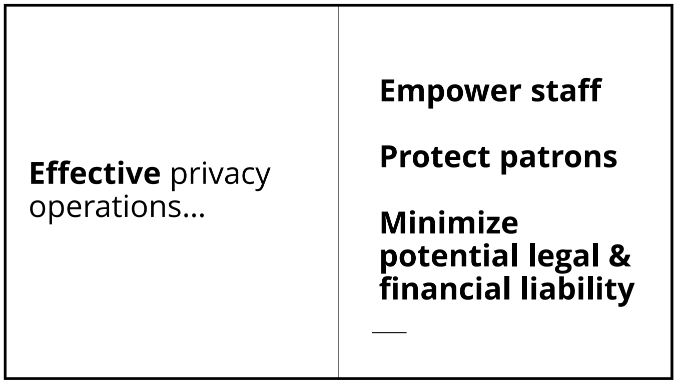


Privacy Operations - Stakeholders

- Library administrators
- Legal counsel
- Library board
- Parent organization/institution
- Library staff
- Patrons
- Community partners
- Professional organizations
- State libraries
- Vendors

Image source – Women In Tech - 65 by WOCinTech Chat, CC BY 2.0, https://www.flickr.com/photos/wocintechchat/22344392878/

11



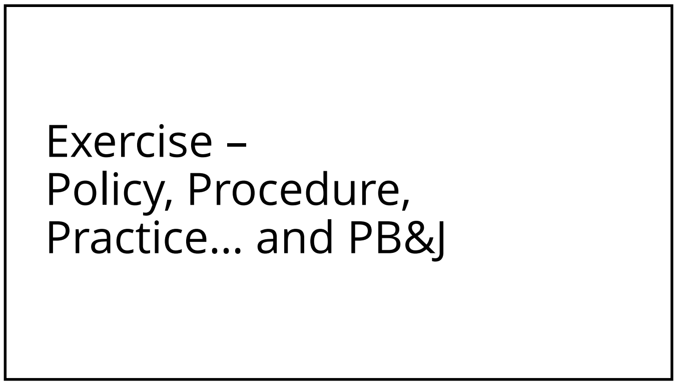
Effective privacy operations…

Empower staff

Protect patrons

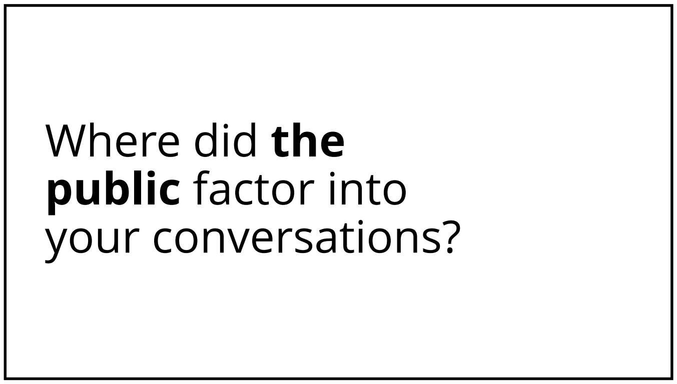
Minimize potential legal & financial liability

12



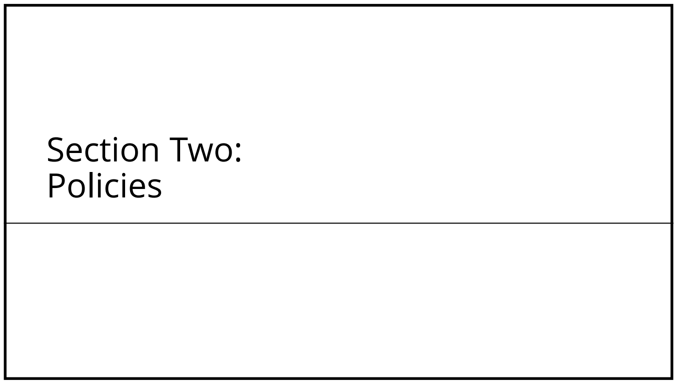
Exercise –
Policy, Procedure,
Practice… and PB&J

13



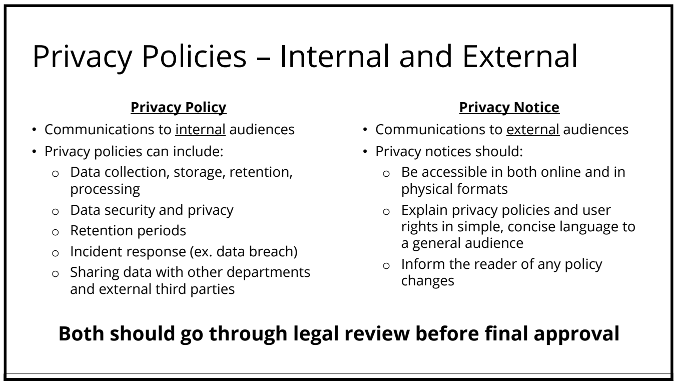
Where did **the public** factor into your conversations?

14



Section Two:
Policies

15



Privacy Policies – Internal and External

Privacy Policy

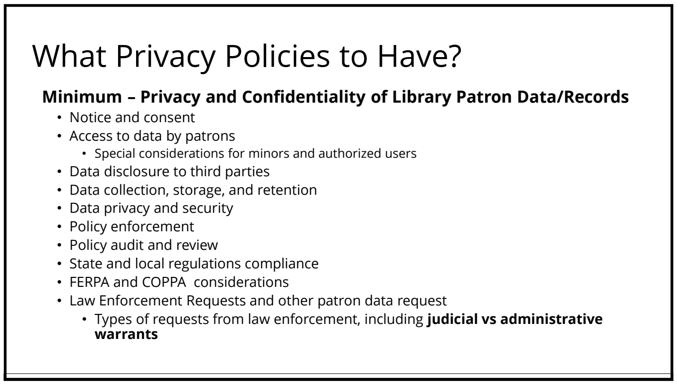
- Communications to internal audiences
- Privacy policies can include:
  - Data collection, storage, retention, processing
  - Data security and privacy
  - Retention periods
  - Incident response (ex. data breach)
  - Sharing data with other departments and external third parties

Privacy Notice

- Communications to external audiences
- Privacy notices should:
  - Be accessible in both online and in physical formats
  - Explain privacy policies and user rights in simple, concise language to a general audience
  - Inform the reader of any policy changes

Both should go through legal review before final approval

16

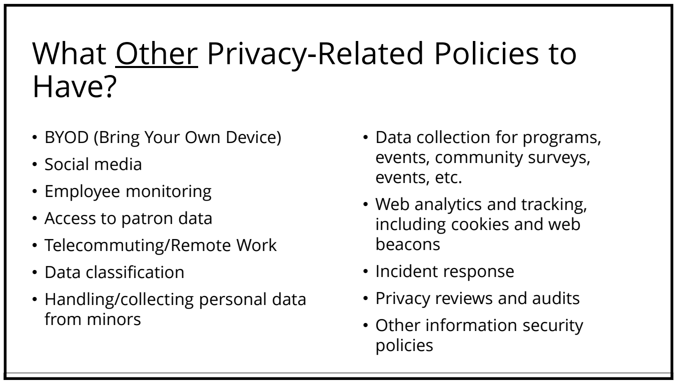


What Privacy Policies to Have?

Minimum – Privacy and Confidentiality of Library Patron Data/Records

- Notice and consent
- Access to data by patrons
  - Special considerations for minors and authorized users
- Data disclosure to third parties
- Data collection, storage, and retention
- Data privacy and security
- Policy enforcement
- Policy audit and review
- State and local regulations compliance
- FERPA and COPPA considerations
- Law Enforcement Requests and other patron data request
  - Types of requests from law enforcement, including **judicial vs administrative warrants**

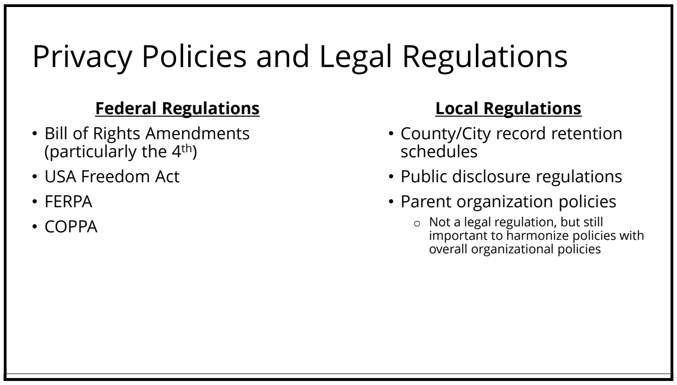
17



What Other Privacy-Related Policies to Have?

- BYOD (Bring Your Own Device)
- Social media
- Employee monitoring
- Access to patron data
- Telecommuting/Remote Work
- Data classification
- Handling/collecting personal data from minors
- Data collection for programs, events, community surveys, events, etc.
- Web analytics and tracking, including cookies and web beacons
- Incident response
- Privacy reviews and audits
- Other information security policies

18



Privacy Policies and Legal Regulations

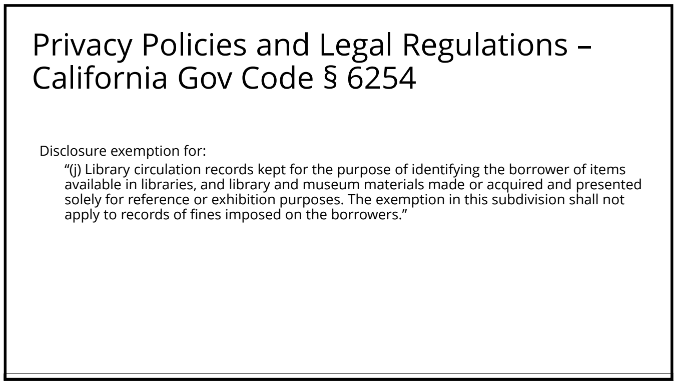
Federal Regulations

- Bill of Rights Amendments (particularly the 4th)
- USA Freedom Act
- FERPA
- COPPA

Local Regulations

- County/City record retention schedules
- Public disclosure regulations
- Parent organization policies
  - Not a legal regulation, but still important to harmonize policies with overall organizational policies

19

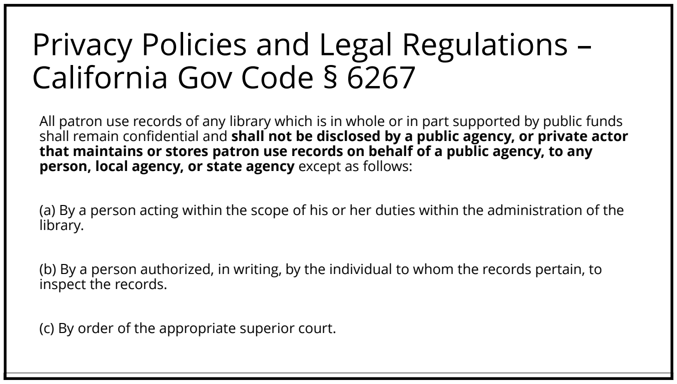


Privacy Policies and Legal Regulations – California Gov Code § 6254

Disclosure exemption for:

> "(j) Library circulation records kept for the purpose of identifying the borrower of items available in libraries, and library and museum materials made or acquired and presented solely for reference or exhibition purposes. The exemption in this subdivision shall not apply to records of fines imposed on the borrowers."

20



Privacy Policies and Legal Regulations – California Gov Code § 6267

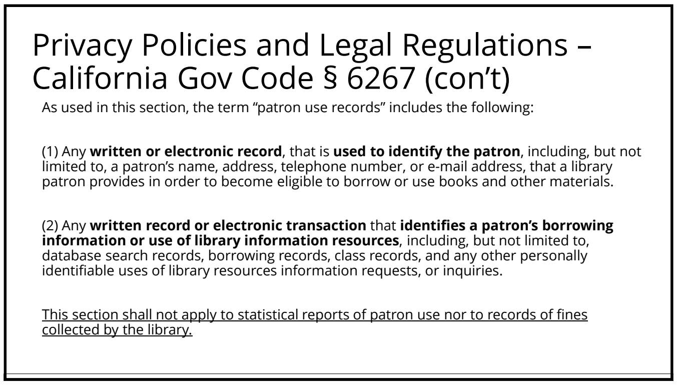
All patron use records of any library which is in whole or in part supported by public funds shall remain confidential and **shall not be disclosed by a public agency, or private actor that maintains or stores patron use records on behalf of a public agency, to any person, local agency, or state agency** except as follows:

(a) By a person acting within the scope of his or her duties within the administration of the library.

(b) By a person authorized, in writing, by the individual to whom the records pertain, to inspect the records.

(c) By order of the appropriate superior court.

21



Privacy Policies and Legal Regulations – California Gov Code § 6267 (con't)

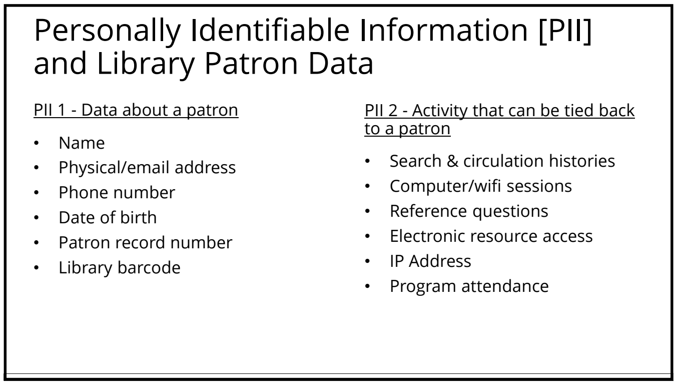
As used in this section, the term "patron use records" includes the following:

(1) Any **written or electronic record**, that is **used to identify the patron**, including, but not limited to, a patron's name, address, telephone number, or e-mail address, that a library patron provides in order to become eligible to borrow or use books and other materials.

(2) Any **written record or electronic transaction** that **identifies a patron's borrowing information or use of library information resources**, including, but not limited to, database search records, borrowing records, class records, and any other personally identifiable uses of library resources information requests, or inquiries.

<u>This section shall not apply to statistical reports of patron use nor to records of fines collected by the library.</u>

22



Personally Identifiable Information [PII] and Library Patron Data

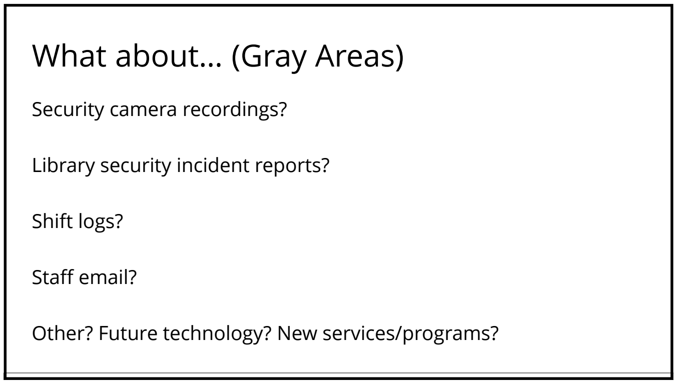
<u>PII 1 - Data about a patron</u>

- Name
- Physical/email address
- Phone number
- Date of birth
- Patron record number
- Library barcode

<u>PII 2 - Activity that can be tied back to a patron</u>

- Search & circulation histories
- Computer/wifi sessions
- Reference questions
- Electronic resource access
- IP Address
- Program attendance

23



What about… (Gray Areas)

Security camera recordings?

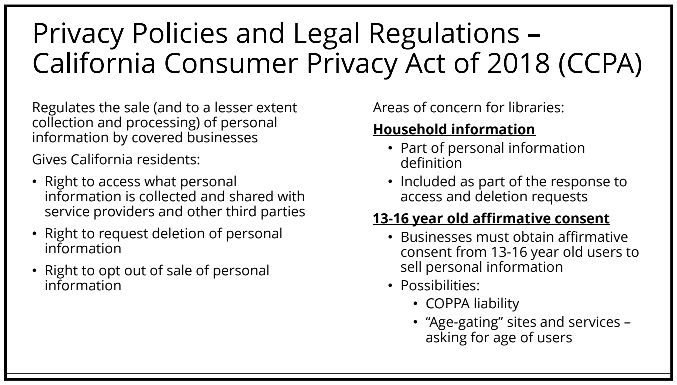
Library security incident reports?

Shift logs?

Staff email?

Other? Future technology? New services/programs?

24



Privacy Policies and Legal Regulations – California Consumer Privacy Act of 2018 (CCPA)

Regulates the sale (and to a lesser extent collection and processing) of personal information by covered businesses

Gives California residents:

- Right to access what personal information is collected and shared with service providers and other third parties
- Right to request deletion of personal information
- Right to opt out of sale of personal information

Areas of concern for libraries:

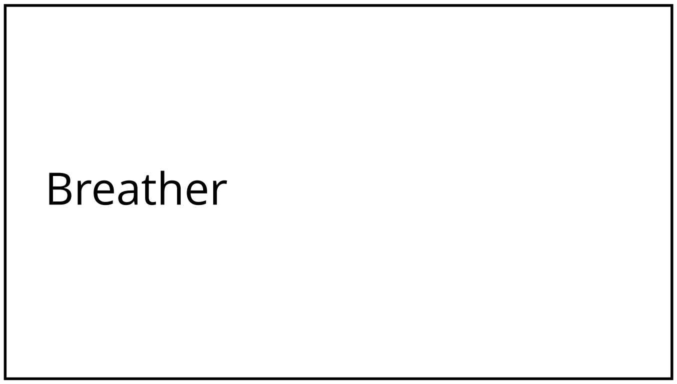
Household information

- Part of personal information definition
- Included as part of the response to access and deletion requests

13-16 year old affirmative consent

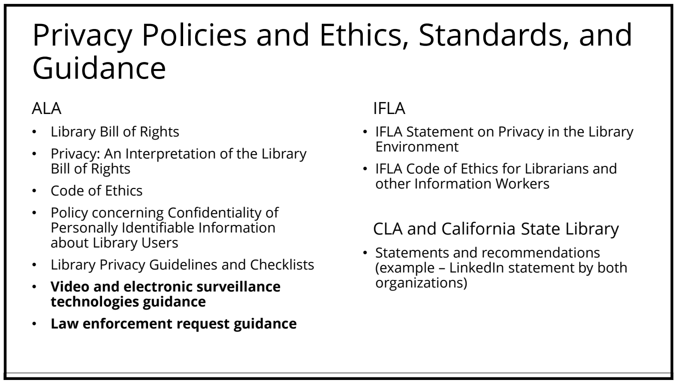
- Businesses must obtain affirmative consent from 13-16 year old users to sell personal information
- Possibilities:
  - COPPA liability
  - "Age-gating" sites and services – asking for age of users

25



Breather

26



Privacy Policies and 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**

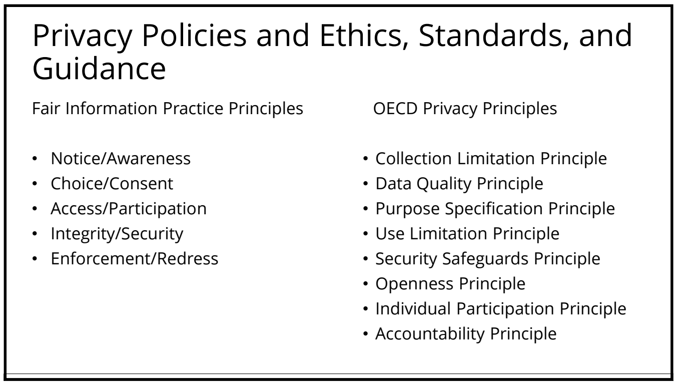
IFLA

- 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)

27



Privacy Policies and Ethics, Standards, and Guidance

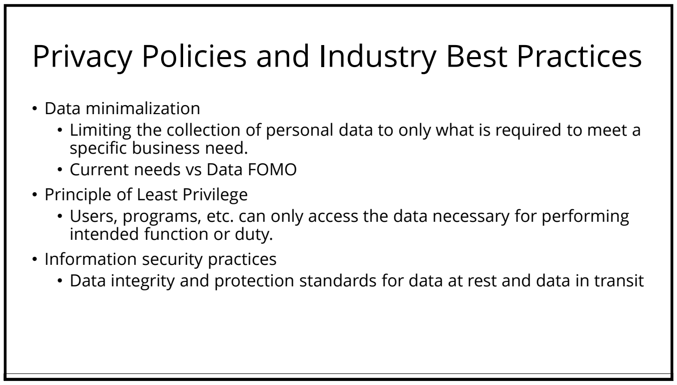
Fair Information Practice Principles

- Notice/Awareness
- Choice/Consent
- Access/Participation
- Integrity/Security
- Enforcement/Redress

OECD Privacy Principles

- Collection Limitation Principle
- Data Quality Principle
- Purpose Specification Principle
- Use Limitation Principle
- Security Safeguards Principle
- Openness Principle
- Individual Participation Principle
- Accountability Principle

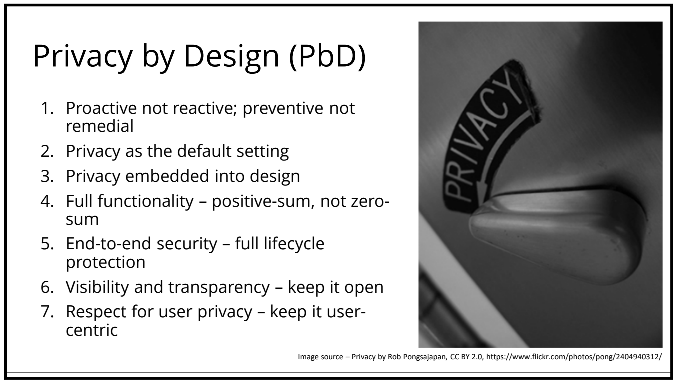
28



Privacy Policies and Industry Best Practices

- Data minimalization
  - Limiting the collection of personal data to only what is required to meet a specific business need.
  - Current needs vs Data FOMO
- Principle of Least Privilege
  - Users, programs, etc. can only access the data necessary for performing intended function or duty.
- Information security practices
  - Data integrity and protection standards for data at rest and data in transit

29



Privacy by Design (PbD)

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

Image source – Privacy by Rob Pongsajapan, CC BY 2.0, https://www.flickr.com/photos/pong/2404940312/

30

Building a Privacy Notice - Elements

- What user data is collected, processed, and retained
- How user data is collected
- Business reasons for collection and processing of user data
- What data is shared with third parties
- Business reasons for sharing user data with third parties
- How users can control collection of data
- How users can control sharing of data with third parties
- How users can access, modify, export, and delete their data
- Who to contact for questions or resolving issues
- Data protection and security
- Effective date of notice
- Changes to notice

31

Notice User Experience and Accessibility

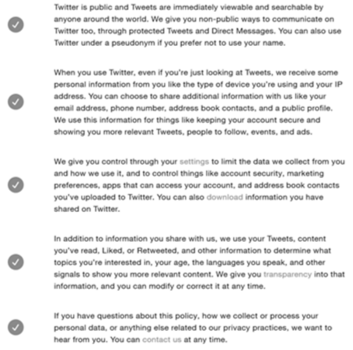
Considerations

- Website content navigation
  - Can your patrons find the privacy notice on the front page of your site?
- Language
  - Jargon vs plain language
  - English as Other Language
- Audience
  - Cultural knowledge assumptions
- Notice accessibility
  - Accessibility standards and design best practices

Strategies

- Focus groups with staff and patrons
- Community listening sessions
- Usability testing – tasks to find and to interpret privacy information on the website
- Accessibility testing
- Translations
- Layered privacy notice design

32



✓ Twitter is public and Tweets are immediately viewable and searchable by anyone around the world. We give you non-public ways to communicate on Twitter too, through protected Tweets and Direct Messages. You can also use Twitter under a pseudonym if you prefer not to use your name.

✓ When you use Twitter, even if you're just looking at Tweets, we receive some personal information from you like the type of device you're using and your IP address. You can choose to share additional information with us like your email address, phone number, address book contacts, and a public profile. We use this information for things like keeping your account secure and showing you more relevant Tweets, people to follow, events, and ads.

✓ We give you control through your settings to limit the data we collect from you and how we use it, and to control things like account security, marketing preferences, apps that can access your account, and address book contacts you've uploaded to Twitter. You can also download information you have shared on Twitter.

✓ In addition to information you share with us, we use your Tweets, content you've read, Liked, or Retweeted, and other information to determine what topics you're interested in, your age, the languages you speak, and other signals to show you more relevant content. We give you transparency into that information, and you can modify or correct it at any time.

✓ If you have questions about this policy, how we collect or process your personal data, or anything else related to our privacy practices, we want to hear from you. You can contact us at any time.

33

Communicating a Privacy Policy to Others

Privacy Policy

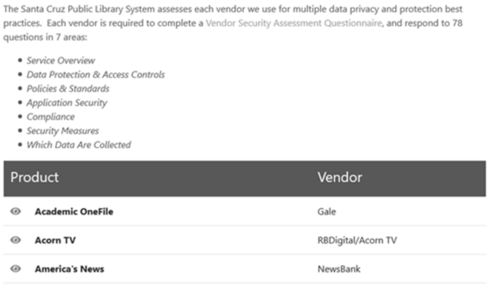
- Staff training
  - Interactive training
  - Refresher trainings
  - Scenario-based training
- Intranet knowledge base for privacy resources and documentation
- Email announcements
- Team meetings

Privacy Notice

- Marketing and Press Releases
- Community outreach
- Physical communication
  - Public posting in conspicuous areas
  - Pamphlets in service population languages
- Electronic communication
  - Direct communication to patrons
  - Website footer/header
  - (Maybe) Website alerts and "Just in Time" Notifications

34

What about vendor privacy notices?



The Santa Cruz Public Library System assesses each vendor we use for multiple data privacy and protection best practices. Each vendor is required to complete a Vendor Security Assessment Questionnaire, and respond to 78 questions in 7 areas:

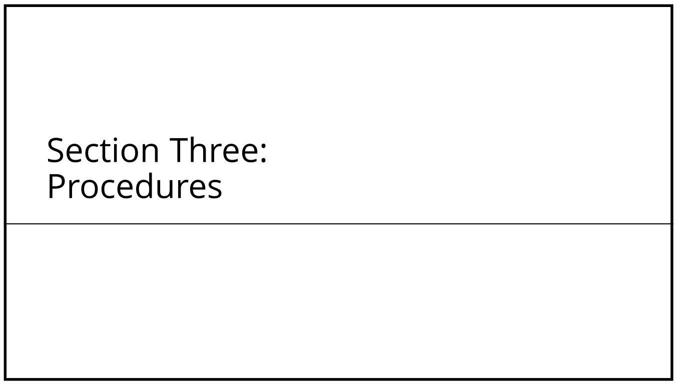
- *Service Overview*
- *Data Protection & Access Controls*
- *Policies & Standards*
- *Application Security*
- *Compliance*
- *Security Measures*
- *Which Data Are Collected*

Product	Vendor
Academic OneFile	Gale
Acorn TV	RBDigital/Acorn TV
America's News	NewsBank

35

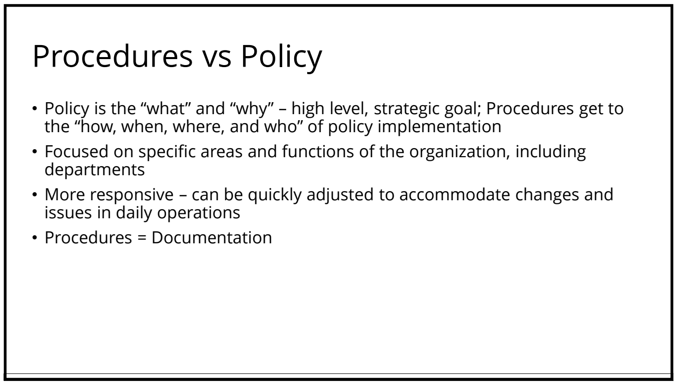
Exercise – Privacy Notice Review

36



Section Three: Procedures

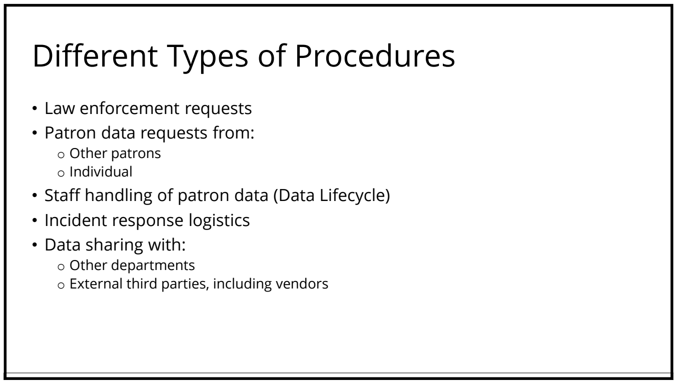
37



Procedures vs Policy

- Policy is the “what” and “why” – high level, strategic goal; Procedures get to the “how, when, where, and who” of policy implementation
- Focused on specific areas and functions of the organization, including departments
- More responsive – can be quickly adjusted to accommodate changes and issues in daily operations
- Procedures = Documentation

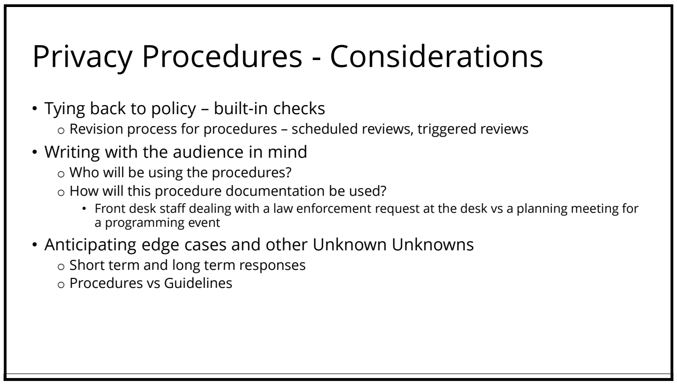
38



Different Types of Procedures

- Law enforcement requests
- Patron data requests from:
  - Other patrons
  - Individual
- Staff handling of patron data (Data Lifecycle)
- Incident response logistics
- Data sharing with:
  - Other departments
  - External third parties, including vendors

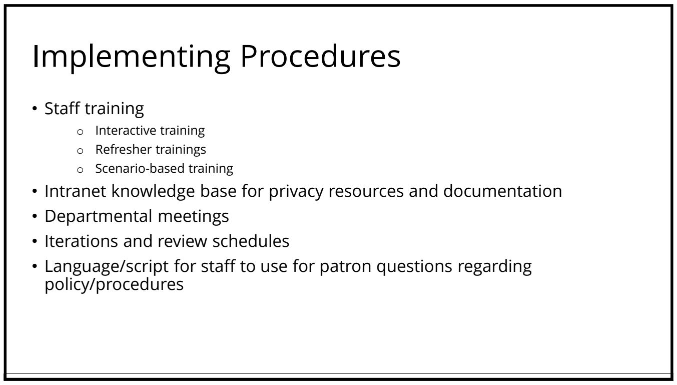
39



Privacy Procedures - Considerations

- Tying back to policy – built-in checks
  - o Revision process for procedures – scheduled reviews, triggered reviews
- Writing with the audience in mind
  - o Who will be using the procedures?
  - o How will this procedure documentation be used?
    - Front desk staff dealing with a law enforcement request at the desk vs a planning meeting for a programming event
- Anticipating edge cases and other Unknown Unknowns
  - o Short term and long term responses
  - o Procedures vs Guidelines

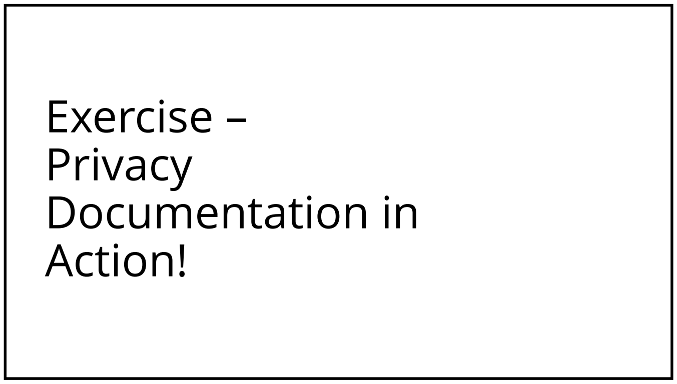
40



Implementing Procedures

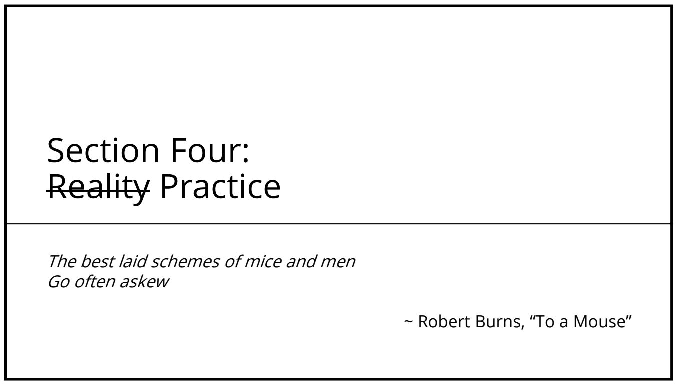
- Staff training
  - o Interactive training
  - o Refresher trainings
  - o Scenario-based training
- Intranet knowledge base for privacy resources and documentation
- Departmental meetings
- Iterations and review schedules
- Language/script for staff to use for patron questions regarding policy/procedures

41



Exercise – Privacy Documentation in Action!

42

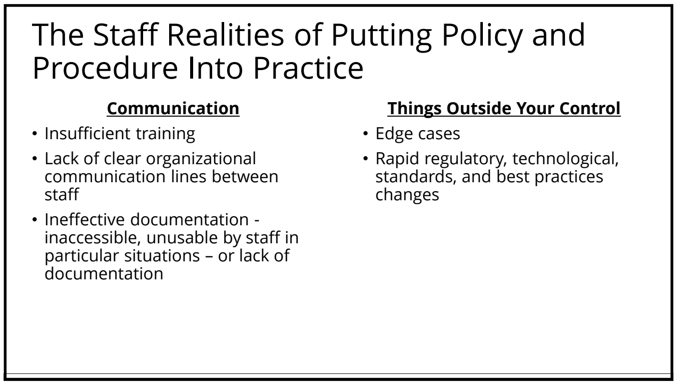


Section Four:
~~Reality~~ Practice

The best laid schemes of mice and men
Go often askew

~ Robert Burns, “To a Mouse”

43



The Staff Realities of Putting Policy and Procedure Into Practice

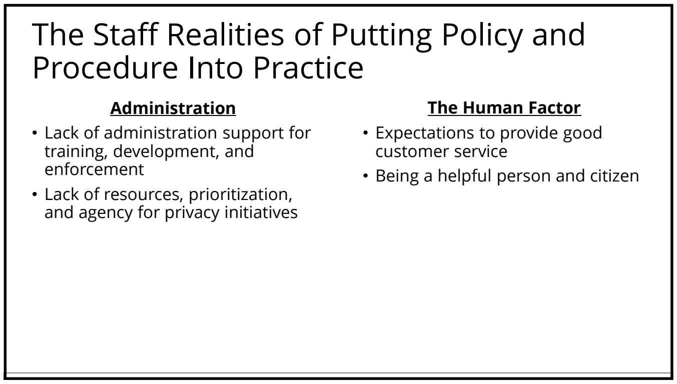
Communication

- Insufficient training
- Lack of clear organizational communication lines between staff
- Ineffective documentation - inaccessible, unusable by staff in particular situations – or lack of documentation

Things Outside Your Control

- Edge cases
- Rapid regulatory, technological, standards, and best practices changes

44



The Staff Realities of Putting Policy and Procedure Into Practice

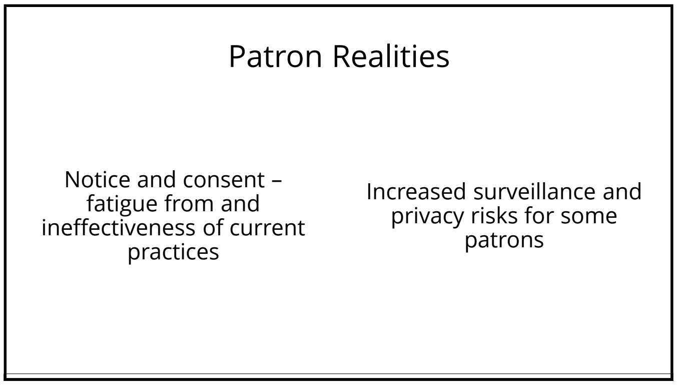
Administration

- Lack of administration support for training, development, and enforcement
- Lack of resources, prioritization, and agency for privacy initiatives

The Human Factor

- Expectations to provide good customer service
- Being a helpful person and citizen

45

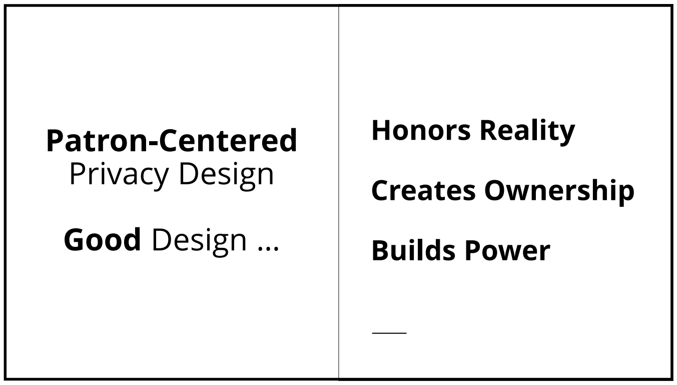


Patron Realities

Notice and consent – fatigue from and ineffectiveness of current practices

Increased surveillance and privacy risks for some patrons

46



Patron-Centered Privacy Design

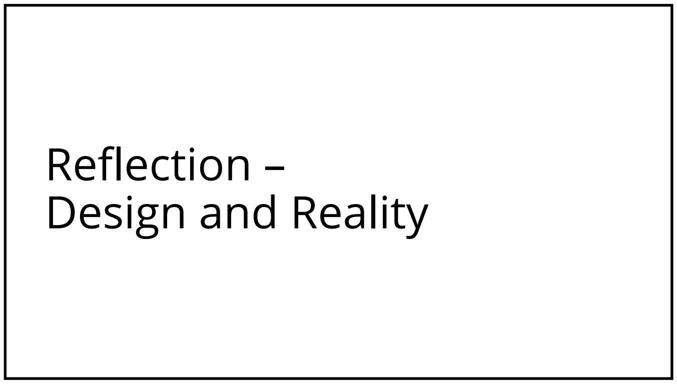
Good Design …

Honors Reality

Creates Ownership

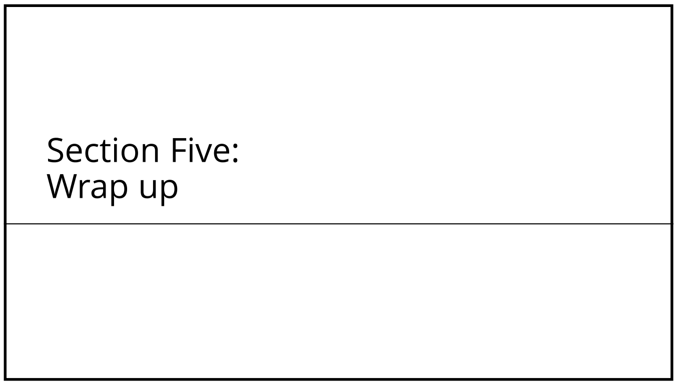
Builds Power

47



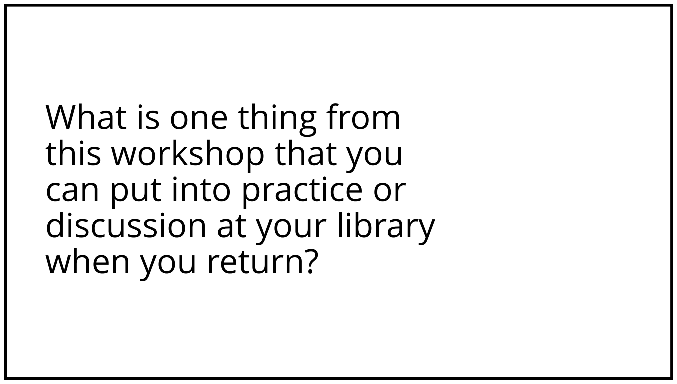
Reflection –
Design and Reality

48



Section Five:
Wrap up

49



What is one thing from this workshop that you can put into practice or discussion at your library when you return?

50

Thank you

:-)

LDH Consulting Services

Becky Yoose
Library Data Privacy Consultant
LDH Consulting Services

Email:
becky@ldhconsultingservices.com

51

Framework Overviews

Fair Information Principles (FIPs/FIPPs)

Text Source: Federal Trade Commission. 2009. “Fair Information Practice Principles.” March 31, 2009. Archived at https://web.archive.org/web/20090331134113/http://www.ftc.gov/reports/privacy3/fairinfo.shtm.

1. Notice/Awareness

The most fundamental principle is notice. Consumers should be given notice of an entity's information practices before any personal information is collected from them. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information. Moreover, three of the other principles discussed below -- choice/consent, access/participation, and enforcement/redress -- are only meaningful when a consumer has notice of an entity's policies, and his or her rights with respect thereto.

While the scope and content of notice will depend on the entity's substantive information practices, notice of some or all of the following have been recognized as essential to ensuring that consumers are properly informed before divulging personal information:

- identification of the entity collecting the data;
- identification of the uses to which the data will be put;
- identification of any potential recipients of the data;
- the nature of the data collected and the means by which it is collected if not obvious (passively, by means of electronic monitoring, or actively, by asking the consumer to provide the information);
- whether the provision of the requested data is voluntary or required, and the consequences of a refusal to provide the requested information; and
- the steps taken by the data collector to ensure the confidentiality, integrity and quality of the data.

Some information practice codes state that the notice should also identify any available consumer rights, including: any choice respecting the use of the data; whether the consumer has been given a right of access to the data; the ability of the consumer to contest inaccuracies; the availability of redress for violations of the practice code; and how such rights can be exercised.

In the Internet context, notice can be accomplished easily by the posting of an information practice disclosure describing an entity's information practices on a company's site on the Web. To be effective, such a disclosure should be clear and conspicuous, posted in a prominent location, and readily accessible from both the site's home page and any Web page where information is collected from the consumer. It should also be unavoidable and understandable so that it gives consumers meaningful and effective notice of what will happen to the personal information they are asked to divulge.

2. Choice/Consent

The second widely-accepted core principle of fair information practice is consumer choice or consent. At its simplest, choice means giving consumers options as to how any personal information collected from them may be used. Specifically, choice relates to secondary uses of information -- *i.e.*, uses beyond those necessary to complete the contemplated transaction. Such secondary uses can be internal, such as placing the consumer on the collecting company's mailing list in order to market additional products or promotions, or external, such as the transfer of information to third parties.

Traditionally, two types of choice/consent regimes have been considered: opt-in or opt-out. Opt-in regimes require affirmative steps by the consumer to allow the collection and/or use of information; opt-out regimes require affirmative steps to prevent the collection and/or use of such information. The distinction lies in the default rule when no affirmative steps are taken by the consumer. Choice can also involve more than a binary yes/no option. Entities can, and do, allow consumers to tailor the nature of the information they reveal and the uses to which it will be put. Thus, for example, consumers can be provided separate choices as to whether they wish to be on a company's general internal mailing list or a marketing list sold to third parties. In order to be effective, any choice regime should provide a simple and easily-accessible way for consumers to exercise their choice.

In the online environment, choice easily can be exercised by simply clicking a box on the computer screen that indicates a user's decision with respect to the use and/or dissemination of the information being collected. The online environment also presents new possibilities to move beyond the opt-in/opt-out paradigm. For example, consumers could be required to specify their preferences regarding information use before entering a Web site, thus effectively eliminating any need for default rules.

3. Access/Participation

Access is the third core principle. It refers to an individual's ability both to access data about him or herself -- *i.e.*, to view the data in an entity's files -- and to contest that data's accuracy and completeness. Both are essential to ensuring that data are accurate and complete. To be meaningful, access must encompass timely and inexpensive access to data, a simple means for contesting inaccurate or incomplete data, a mechanism by which the data collector can verify the information, and the means by which corrections and/or consumer objections can be added to the data file and sent to all data recipients.

4. Integrity/Security

The fourth widely accepted principle is that data be accurate and secure. To assure data integrity, collectors must take reasonable steps, such as using only reputable sources of data and cross-referencing data against multiple sources, providing consumer access to data, and destroying untimely data or converting it to anonymous form.

Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data. Managerial measures include internal organizational measures that limit access to data and ensure that those individuals with access do not utilize the data for unauthorized purposes. Technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and the storage of data on secure servers or computers that are inaccessible by modem.

5. Enforcement/Redress

It is generally agreed that the core principles of privacy protection can only be effective if there is a mechanism in place to enforce them. Absent an enforcement and redress mechanism, a fair information practice code is merely suggestive rather than prescriptive, and does not ensure compliance with core fair information practice principles. Among the alternative enforcement approaches are industry self-regulation; legislation that would create private remedies for consumers; and/or regulatory schemes enforceable through civil and criminal sanctions.

a. Self-Regulation

To be effective, self-regulatory regimes should include both mechanisms to ensure compliance (enforcement) and appropriate means of recourse by injured parties (redress). Mechanisms to ensure compliance include making acceptance of and compliance with a code of fair information practices a condition of membership in an industry association; external audits to verify compliance; and certification of entities that have adopted and comply with the code at issue. A self-regulatory regime with many of these principles has recently been adopted by the individual reference services industry.

Appropriate means of individual redress include, at a minimum, institutional mechanisms to ensure that consumers have a simple and effective way to have their concerns addressed. Thus, a self-regulatory system should provide a means to investigate complaints from individual consumers and ensure that consumers are aware of how to access such a system.

If the self-regulatory code has been breached, consumers should have a remedy for the violation. Such a remedy can include both the righting of the wrong (e.g., correction of any misinformation, cessation of unfair practices) and compensation for any harm suffered by the consumer. Monetary sanctions would serve both to compensate the victim of unfair practices and as an incentive for industry compliance. Industry codes can provide for alternative dispute resolution mechanisms to provide appropriate compensation.

OECD Privacy Principles

Text Source: OECD (2013), The OECD Privacy Framework, https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm.

1. Collection Limitation Principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3. Purpose Specification Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use Limitation Principle

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or

b) by the authority of law.

5. Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

6. Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. Individual Participation Principle

An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him

i) within a reasonable time;
ii) at a charge, if any, that is not excessive;
iii) in a reasonable manner; and
iv) in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

8. Accountability Principle

A data controller should be accountable for complying with measures which give effect to the principles stated above.

Privacy by Design

Seven Foundational Principles

Text Source: Cavoukian, Ann. 2011. “Privacy by Design: The 7 Foundational Principles.” Information and Privacy Commissioner of Ontario. https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

1. Proactive not reactive; preventive not remedial

The privacy by design approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. Privacy by design does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to prevent them from occurring. In short, privacy by design comes before-the-fact, not after.

2. Privacy as the default

Privacy by design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default.

3. Privacy embedded into design

Privacy by design is embedded into the design and architecture of IT systems as well as business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system without diminishing functionality.

4. Full functionality – positive-sum, not zero-sum

Privacy by design seeks to accommodate all legitimate interests and objectives in a positive-sum “win-win” manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by design avoids the pretense of false dichotomies, such as privacy versus security, demonstrating that it is possible to have both.

5. End-to-end security – full lifecycle protection

Privacy by design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, privacy by design ensures cradle-to-grave, secure lifecycle management of information, end-to-end.

6. Visibility and transparency – keep it open

Privacy by design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. Respect for user privacy – keep it user-centric

Above all, privacy by design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

Annotated Example Privacy Policies and Notices Bibliography

Disclaimer – the policies included in this document are for informational purposes only and do not necessarily reflect all privacy notice and policy best practices. Please consult with legal counsel for legal advice or questions regarding any of the resources in this document.

Non-Library Examples

BBC

https://www.bbc.co.uk/usingthebbc/privacy/

What to look for:

- Use of plain language
- Layered privacy notice design – the BBC privacy landing page leads the user to other pages in the privacy site. This approach can help limit the information posted on a single page, but those who decide to take this approach should also allow the user to navigate with minimal effort between layers in the site.

Twitter

https://twitter.com/en/privacy

What to look for:

- Use of plain language
- Layered privacy notice design – Twitter's layering is all on one page, with the summary on top of the page. This is a mobile-friendly design approach that is responsive to multiple screen sizes. Twitter also places a static navigational menu on the top right of the page for users to jump between sections.

Library Examples

Cleveland Heights-University Heights Public Library

https://heightslibrary.org/services/privacy-statement/

What to look for:

- Steps through instances where patron information might be disclosed, including law enforcement requests, emergencies, and patron requests for information, using clear, plain language
- Lists personal information collected by the library
- Provides contact information for questions
- Links to additional resources (Public Records Policy)

Hennepin County Library

https://www.hclib.org/about/policies/patron-data-privacy and https://www.hclib.org/about/policies/disclosing-patron-data-staff-and-volunteer-responsibilities

What to look for:

- Different types of policies – A general Policy about patron data and an Administrative Policy describing the responsibilities ("how" and "who") of the library in implementing the general policy
    - This approach allows for providing details to the public about the library's approach to privacy without leaning heavily on the general privacy notice to convey this information. Having administrative policies available to the public also provides transparency on the library's privacy practices.
- Integrates and links to relevant parent organization policies and legal regulations that are related to privacy policy
- Includes scope and applicability of policy
- Includes review process details, as well as dates for past and future renewals

Indiana University Libraries

https://policies.iu.edu/policies/lib-01-libraries-privacy/index.html

What to look for:

- Section with details about policy creation, revision, contacts, feedback, and governance over policy enforcement
- Includes scope and applicability of policy
- Integrates and links to relevant parent organization policies that are related to privacy policy
- Clear document outline structure
- Details about third party analytics software use by the library

New York Public Library

https://www.nypl.org/help/about-nypl/legal-notices/privacy-policy

What to look for:

- Dedicated pages for translations of the policy in several languages
- Date of last update at the beginning of the policy
- Follows industry best practices for structure and content, including describing how the library obtains patron data through various methods, when patron data is shared or disclosed to third parties
- Separate section for minors, including information about how parents and guardians can access their children's information
- Provides dedicated contact for privacy questions
- Provides links to opt-out of data sharing for fundraising and marketing purposes

- Provides contact information for patrons who want to access what data NYPL has on file

Extra:

- NYPL published a blog post for their patrons to read about the major update of the privacy policy - https://www.nypl.org/help/about-nypl/legal-notices/privacy-policy/intro

Multnomah County Library

https://multcolib.org/privacy-and-confidentiality-library-records

What to look for:

- Section dedicated to third party vendors used by the library who collect and/or disclose patron information
- Describes how the library obtains patron data through various methods and when patron data is shared or disclosed to third parties

San Francisco Public Library

https://sfpl.org/about/privacy-policy

What to look for:

- General summary of notice in beginning of document
- Section dedicated to third party discovery layer used by the library that collects and/or discloses patron information
- Details about RFID use by the library
- Details about information transmitted through email and web forms
- Details about handling information from reference questions
- Integrates and links to relevant parent organization policies and legal regulations that are related to privacy policy

Extra:

- SFPL includes three additional documents that provide patrons with privacy information: two FAQs and a privacy inventory. FAQs are a good format to provide ready answers for staff as well as patrons. The privacy inventory is a summary of a data inventory, and provides transparency into what the library collects and stores, as well as who has access and when the data is deleted. While all three documents are good additions to the privacy notice, the PDF-only publication of these documents limits their discoverability, as well as introduces some accessibility and preservation issues. Providing dedicated web pages for each document’s content will allow for better indexing by search engines, including the library website’s own search engine.

San Jose Public Library

https://www.sjpl.org/privacy-policy

What to look for:

- Integrates and links to relevant organizations' policies that are related to the library's privacy policy
- Lists personal information collected by the library
- Provides contact information for questions
- Details about third party analytics software use by the library
- Details about RFID use by the library
- Section dedicated to third party vendors used by the library who collect and/or disclose patron information
- Section about surveillance technologies at the library

Library Vendor Privacy Notices Examples

The following examples are dedicated public pages for patrons to learn more about vendor privacy practices. Each example has its own workflow and process in adding and maintaining the vendor list of privacy notices. The best practices around these pages are still a work in progress in the library field. Nonetheless, libraries should follow usability, accessibility, and design best practices when creating vendor privacy notices pages.

San Jose Public Library

https://www.sjpl.org/vendor-privacy-policies

Santa Cruz Public Library

https://www.santacruzpl.org/data_privacy/

York University Libraries

https://www.library.yorku.ca/web/collections/vendor-policies/

References and Further Reading

General

Aye, George. 2019. “Why Is Good Design So Hard to Do?” October 3, 2019. https://www.tamarackcommunity.ca/hubfs/Events/Multi-Day%20Events/2019%20CCF%20Vancouver/Resource%20Uploads/2019%20CCF%20Keynote%20-%20George%20Aye.pdf?hsLang=en.

ComplianceBridge Policies & Procedures Team. 2017. “Policy vs Procedures - Understanding The Key Difference.” *ComplianceBridge* (blog). June 28, 2017. http://compliancebridge.com/policy-vs-procedures/.

Cronk, R. Jason. 2020. “Exploring Privacy Values.” January 8, 2020. https://iapp.org/news/a/exploring-privacy-values/.

Davis, Ben. 2020. “GDPR: How to Create Best Practice Privacy Notices - Econsultancy.” Econsultancy. July 17, 2020. https://econsultancy.com/gdpr-best-practice-privacy-notices-examples/.

Information Commissioner’s Office. 2019. “What Methods Can We Use to Provide Privacy Information?” ICO. October 8, 2019. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/.

Kinsella Media, LLC. n.d. “Plain Language Primer for Privacy Policies.” Accessed January 12, 2020. https://iapp.org/media/pdf/knowledge_center/Privacy_Policy_Primer.pdf.

Litman-Navarro, Kevin. 2019. “Opinion | We Read 150 Privacy Policies. They Were an Incomprehensible Disaster.” *The New York Times*, June 12, 2019, sec. Opinion. https:/www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html.

Magi, T., M. Garnar, and O.I. Freedom. 2015. *Intellectual Freedom Manual, Ninth Edition*. American Library Association.

Marden, William. 2017. “The Path to a Creating a New Privacy Policy: NYPL’s Story.” *Choose Privacy Every Day* (blog). May 1, 2017. https://chooseprivacyeveryday.org/the-path-to-a-creating-a-new-privacy-policy/.

Newman, Bobbi, and Bonnie Tijerina, eds. *Protecting Patron Privacy: A LITA Guide*. Rowman & Littlefield, 2017.

Mid-Hudson Library System. n.d. “Policies.” Accessed January 12, 2020. https://midhudson.org/topics/director-resources/policies/.

Saint Louis University Information Technology Services : SLU. n.d. “Policies, Standards, Guidelines, Procedures/Processes.” Accessed January 12, 2020. https://www.slu.edu/its/policies.

AASL Resources

AASL. 2006. “Position Statement on the Confidentiality of Library Records.” American Association of School Librarians (AASL). September 27, 2006. http://www.ala.org/aasl/advocacy/resources/statements/library-records.

ALA Resources

ALA. 2006a. “Policy Concerning Confidentiality of Personally Identifiable Information about Library Users.” Advocacy, Legislation & Issues. July 7, 2006. http://www.ala.org/advocacy/intfreedom/statementspols/otherpolicies/policyconcerning.

———. 2006b. “Resolution on the Retention of Library Usage Records.” Accessed April 10, 2018. http://www.ala.org/Template.cfm?Section=ifresolutions&Template=/ContentManagement/ContentDisplay.cfm&ContentID=135888.

———. 2007a. “Intellectual Freedom and Censorship Q & A.” Advocacy, Legislation & Issues. Accessed October 12, 2019. http://www.ala.org/advocacy/intfreedom/censorship/faq.

———. 2007b. “Privacy and Confidentiality Q&A.” Text. Advocacy, Legislation & Issues. May 29, 2007. http://www.ala.org/advocacy/intfreedom/privacyconfidentialityqa.

———. 2007c. “Privacy Tool Kit.” Text. Advocacy, Legislation & Issues. http://www.ala.org/advocacy/privacy/toolkit.

———. 2007d. “State Privacy Laws Regarding Library Records.” Advocacy, Legislation & Issues. Accessed June 12, 2019. http://www.ala.org/advocacy/privacy/statelaws.

———. 2008. “Professional Ethics.” Tools, Publications & Resources. Accessed October 12, 2019. http://www.ala.org/tools/ethics.

———. 2009. “United for Libraries Sample Library Policies.” Text. United for Libraries. June 14, 2009. http://www.ala.org/united/trustees/policies.

———. 2017a. “Library Privacy Checklists.” Advocacy, Legislation & Issues. Accessed June 12, 2019. http://www.ala.org/advocacy/privacy/checklists.

———. 2017b. “Library Privacy Guidelines.” Advocacy, Legislation & Issues. Accessed June 12, 2019. http://www.ala.org/advocacy/privacy/guidelines.

———. 2017c. “Suggested Guidelines: How to Respond to Law Enforcement Requests for Library Records and User Information.” Advocacy, Legislation & Issues. Accessed June 12, 2019. http://www.ala.org/advocacy/privacy/lawenforcement/guidelines.

———. 2019a. “Library Bill of Rights.” Advocacy, Legislation & Issues. Accessed October 12, 2019. http://www.ala.org/advocacy/intfreedom/librarybill.

———. 2019b. “Privacy: An Interpretation of the Library Bill of Rights.” Advocacy, Legislation & Issues. Accessed October 12, 2019. http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy.

———. n.d. “LibGuides: Library Policy Development: General.” Accessed January 12, 2020a. //libguides.ala.org/librarypolicy/general.

———. n.d. “LibGuides: Safety and Security in Libraries: Home.” Accessed January 12, 2020b. //libguides.ala.org/safety-security/home.

———. “Students & Minors.” n.d. *Choose Privacy Week*. Accessed April 10, 2018. https://chooseprivacyweek.org/resources/students-and-minors/.

IFLA Resources

IFLA. n.d. “IFLA Code of Ethics for Librarians and Other Information Workers (Full Version).” Accessed January 12, 2020a. https://www.ifla.org/publications/node/11092?og=30.

———. n.d. “IFLA Statement on Privacy in the Library Environment.” Accessed January 12, 2020b. https://www.ifla.org/publications/node/10056.

California Law Resources

"California Consumer Privacy Act (CCPA)." 2018. State of California - Department of Justice - Office of the Attorney General. October 15, 2018. https://www.oag.ca.gov/privacy/ccpa.

"California Government Code § 6254. Records Exempt from Disclosure Requirements." Accessed December 23, 2019. 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." Accessed December 23, 2019. https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=6267.&lawCode=GOV.

California State Library. 2019. "California Library Laws." 2019. https://www.library.ca.gov/services/to-libraries/library-laws/.

Determann, Lothar. 2019. "Analysis: The California Consumer Privacy Act of 2018." International Association of Privacy Professionals. Accessed June 13, 2019. https://iapp.org/news/a/analysis-the-california-consumer-privacy-act-of-2018/.

Schiff, Allison. 2019. "California Gov. Newsom Signs 7 CCPA-Related Bills Into Law." AdExchanger. Accessed October 14, 2019. https://adexchanger.com/privacy/california-gov-newsom-signs-7-ccpa-bills-into-law/.

Industry Standards

Cavoukian, Ann. 2011. "Privacy by Design: The 7 Foundational Principles." Information and Privacy Commissioner of Ontario. https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

Federal Trade Commission. 2009. "Fair Information Practice Principles." March 31, 2009. Archived at https://web.archive.org/web/20090331134113/http://www.ftc.gov/reports/privacy3/fairinfo.shtm.

Garfinkel, Simson L. 2015. “De-Identification of Personal Information.” NIST Interagency/Internal Report (NISTIR) - 8053. National Institute of Standards and Technology. https://www.nist.gov/publications/de-identification-personal-information.

Kissel, Richard, Andrew Regenscheid, Matthew Scholl, and Kevin Stine. 2014. “Guidelines for Media Sanitization.” NIST SP 800-88r1. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-88r1.

McCallister, E, T Grance, and K A Scarfone. 2010. “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).” NIST SP 800-122. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-122.

NIST. 2017. “Section 8 - Privacy Considerations.” NIST SP 800-63. National Institute of Standards and Technology. Accessed January 12, 2020. https://pages.nist.gov/800-63-3/sp800-63a/sec8_privacy.html#genProofReqs.

NIST. 2018. “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.” NIST CSWP 04162018. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018.

NIST. 2020. “NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management”. Version 1.0. Accessed January 20, 2020. https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf.

OECD. 2013. “OECD Privacy Guidelines.” OECD. http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm.

SANS Institute. 2013. “20 Critical Security Controls.” Archived at https://web.archive.org/web/20131101135802/http://www.sans.org/critical-security-controls/spring-2013-poster.pdf.

State of California GOVERNMENT CODE

Section 6254 (excerpt)

6254. Except as provided in Sections 6254.7 and 6254.13, this chapter does not require the disclosure of any of the following records:

…

(j) Library circulation records kept for the purpose of identifying the borrower of items available in libraries, and library and museum materials made or acquired and presented solely for reference or exhibition purposes. The exemption in this subdivision shall not apply to records of fines imposed on the borrowers.

(Amended by Stats. 2019, Ch. 25, Sec. 1. (SB 94) Effective June 27, 2019.)

State of California GOVERNMENT CODE

Section 6267

6267. All patron use records of any library which is in whole or in part supported by public funds shall remain confidential and shall not be disclosed by a public agency, or private actor that maintains or stores patron use records on behalf of a public agency, to any person, local agency, or state agency except as follows:

(a) By a person acting within the scope of his or her duties within the administration of the library.
(b) By a person authorized, in writing, by the individual to whom the records pertain, to inspect the records
(c) By order of the appropriate superior court.

As used in this section, the term “patron use records” includes the following:

(1) Any written or electronic record, that is used to identify the patron, including, but not limited to, a patron’s name, address, telephone number, or e-mail address, that a library patron provides in order to become eligible to borrow or use books and other materials.
(2) (2) Any written record or electronic transaction that identifies a patron’s borrowing information or use of library information resources, including, but not limited to, database search records, borrowing records, class records, and any other personally identifiable uses of library resources information requests, or inquiries.
(3) This section shall not apply to statistical reports of patron use nor to records of fines collected by the library.

(Amended by Stats. 2011, Ch. 80, Sec. 1. (SB 445) Effective January 1, 2012.)