A Practical Guide to Privacy Audits

Presented by Erin Berman & Julie Oborny
San José Public Library
Choose Privacy Week 2018
May 1-7, 2018

Web and social media graphics:
https://chooseprivacyweek.org/programs/web-banners-icons/

Programming resources:
https://chooseprivacyweek.org/programs/programming-in-a-box/

**CPW Online Forum, May 1-7:** Learn more about: Libraries as Private Spaces: Patron Privacy and Data Storage: Balancing Customer Service with Privacy: The Ethical Role of Libraries and Big Data: Helping People Make Realistic Privacy Choices for their Real Lives: Privacy and Google Analytics
Today’s speakers

Julie Oborny, Web Librarian
San Jose Public Library

Erin Berman, Innovations Manager
San Jose Public Library

#chooseprivacy  Choose Privacy Week (May 1 - 7, 2018)
At the end of this session, you will...

1. Understand the basics of privacy ethics within the library profession and its history.
2. Be able to communicate why privacy in the library is important.
3. Know what an internal privacy audit is.
4. Have a guide to start your privacy audit right away.
5. Be able to “sell” the importance of a privacy audit to your administration.
Ethics

- **ALA Code of Ethics**
  - “*We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted.*”

- **Privacy: an Interpretation of the Library Bill of Rights (2002):**
  - “*The American Library Association affirms that rights of privacy are necessary for intellectual freedom and are fundamental to the ethics and practice of librarianship.*”

@mohawklibrarian  @juliedecimal  @PRIVACYALA  #chooseprivacy  Choose Privacy Week  (May 1 - 7, 2018)
History

- Section 215 of the Patriot Act
  - The Librarians’ Version of Section 31.
    Section 215 was supposed to be a sunset provision to allow for bending prior rules that protected privacy and confidentiality and was supposed to expire with the assumption that imminent threats would be gone. Section 31 operates under the premise of imminent threat, as well, and rights can come under threat for both. (See, we tried to throw in a space reference there!)
Why is this important?

“Privacy is essential to the exercise of free speech, free thought, and free association. Lack of privacy and confidentiality chills users' choices, thereby suppressing access to ideas. The possibility of surveillance, whether direct or through access to records of speech, research and exploration, undermines a democratic society.”

- Privacy: An Interpretation of the Library Bill of Rights
What is an audit?

**Definition**: “A technique for assuring that an organization's goals and promises of privacy and confidentiality are supported by its practices, thereby protecting confidential information from abuse and the organization from liability and public relations problems.”
“YOUR SCIENTISTS WERE SO PREOCCUPIED WITH WHETHER THEY COULD THEY DIDN’T STOP TO THINK IF THEY SHOULD.”

—DR. IAN MALCOLM

How much information SHOULD your library and its partners collect?
“We have all the problems of a major theme park and a major zoo, and the computer's not even on its feet yet.” -Ray Arnold, *Jurassic Park*
A privacy audit provides a library opportunity to examine:

- how privacy matters are handled at all levels;
- the flow and storage of data;
- the role data plays within the organization;
- staff training about privacy matters;
- existing and needed privacy policies.

REMEMBER: This is a process, not a one-shot project, AND it will scale differently, depending on your library.
Why is it important?

- Formal Process (Thanks, ALA!)
- Identifying what you are doing well
- Identifying what you need to improve
- Empowering staff
- Empowering your community

And now, all of that summed up in Star Trek quotes ...
"Humans do have an amazing capacity for believing what they choose -- and excluding that which is painful." Mr. Spock, "And The Children Shall Lead"
"You know the greatest danger facing us is ourselves, and irrational fear of the unknown. There is no such thing as the unknown. Only things temporarily hidden, temporarily not understood." James T. Kirk, "The Corbomite Maneuver"
"A library serves no purpose unless someone is using it." Mr. AtoZ, "All Our Yesterdays"
Alright, one quote from an awesome someone who was on that other franchise ...

“Stay afraid, but do it anyway. What’s important is the action. You don’t have to wait to be confident. Just do it and eventually the confidence will follow.”

-Carrie Fisher
How to Perform a Privacy Audit
Step 1:

Review ALA’s Privacy Toolkit

http://www.ala.org/advocacy/privacy/toolkit

- Privacy & the Law
- Privacy Principles
- Writing a Privacy Policy
- Privacy Audits
- Implementing Policies and Procedures
- Talking Points
- Answering Tough Questions
- What ALA is Doing
Step 2:

Getting Buy-In

Speaking with stakeholders and administration

Potential Stakeholders

- Management Team
- Marketing & Communications Department
- Governing Organization (City Council, Board)
- Appropriate Staff e.g. Web, IT, Security, Access, Technical Services, Volunteer Services
- Vendors
Step 3:

Get Comfy With ALA’s Privacy Guidelines

http://www.ala.org/advocacy/privacy/guidelines

- E-book Lending and Digital Content Vendors
- Data Exchange Between Networked Devices and Services
- Public Access Computers and Networks
- Library Websites, OPACs, and Discovery Services
- Library Management Systems
- Students in K-12 Schools
Step 4:

Using the IFC & LITA Checklists

- Priority 1 - Actions that hopefully all libraries can take to improve privacy practices.
- Priority 2 & 3 - Actions that may be more difficult for libraries to implement depending on their technical expertise, available resources, and organizational structure.

http://www.ala.org/advocacy/privacy/checklists
Step 4a:

Making the Checklists Work for Your Library

- Which level will your library strive for?
- Who is responsible?
- What departments/units are missing?
- What items will your library not be implementing? Why not?
Step 4a:

Making the Checklists Work for Your Library

### Priority 1 Actions

1. Create a policy that addresses the collection of patron information. Such a policy should specify that the library is not collecting more patron information than what it needs and that it is not keeping the personally identifiable information of patrons longer than what is necessary.
   - a. Create a privacy policy that is understandable by a layperson.
   - b. Make sure the privacy policy is posted in the library where the public can see it.
   - c. Ensure that the privacy policy includes information about what information the library is tracking, why, and for how long the data is kept.
   - d. Ensure that the privacy policy includes when patron information can be shared and under what conditions.

2. Destroy all paper records with user data, such as computer sign-in sheets.

3. Ensure all existing security certificates for HTTP/SSL are valid and create a procedure for revalidating them annually.

4. Designate a Library Privacy Officer to handle requests for personally identifiable information of patrons from law enforcement officials and other third parties.

### Priority 2 Actions

1. Ensure there is a formal process in place to address breaches of patron data directly under library control or maintained by third parties. The library should notify affected users when they become aware of a breach.

2. Encrypt all user data with secure algorithms in all network and application communications.

3. Purge search history records regularly, ideally when the individual computer session ends.

---

**Excel:** [sjpl.org/privacy-audit-excel](http://sjpl.org/privacy-audit-excel)
(download, 27.55 KB)

**Google:** [sjpl.org/privacy-audit-google](http://sjpl.org/privacy-audit-google)
(online)
Step 5:
Performing the Audit

- Build a timeline
- Assign tasks
- Work with unit managers to review, assess, and implement
- Ask:
  - What information do you collect?
  - Why and how do you collect it?
  - Do you need to collect it?
  - Storage and retention policies/procedures?
  - Unit’s best practices and policies
- Make recommendations
Step 6: Telling the Story

- Department White Papers
  - What information is collected?
  - Where is information collected?
  - How is that information used?
  - What are the storage and retention policies/procedures for customer data?
  - Is information shared with 3rd party vendors? - Who? What? Is it necessary? What are their privacy policies?
  - Current procedures
  - Upcoming changes or recommendations
  - Disseminating
Format the Department White Papers

**ALA Checklist Items**

1. Encrypt all customer data with secure algorithms in all network and application communications.
   a. All network traffic is not currently encrypted, though portions of our network are physically separated, logically separated, and some client/server connections are encrypted. (Needs Work)

**Library Information Technology Privacy Audit**

2. Purge search history records regularly, ideally when the individual computer session ends.
   a. At the end of each individual computer session, reboots are forced by our Reserve-A-Computer program. All public computers wipe all changes made by the customer each time the computer is rebooted. There are no local search history records available after a customer leaves our workstations. (Accomplished)

3. Establish minimum security practices for devices and services.
   a. Library IT has minimum security practices for all servers, workstations, databases, services, and network equipment. (Accomplished)

   a. It is the LIT’s policy to change all default passwords for any system installed on our network. However, passwords used by generic accounts are often left in place by staff for long periods of time, producing the same type of vulnerability. (Needs Work)

5. Disable remote access to the supervisor account (i.e. root or administrator)

---

**Volunteer Services Privacy Audit**

**Volunteer Services Overview**

The Volunteer Services Department collects information from volunteers as they apply in order to screen applicants, track volunteer contributions, and report the number of volunteers and volunteer hours contributed to the library.

**What information do we collect?**

Our department collects personally identifiable information in order to process volunteers into the library system. The information collected allows the library to do background checks on volunteers, to assist the volunteer coordinators at branches in assigning volunteers to different tasks, and for Volunteer Away Your Fines events. Only the necessary information to conduct regular business operations is collected. Personal information collected may include:

- First and last name
- Mailing address
- Email
- Phone number
- Age range (13+, 15+, 18+, 21+, or 50+)
- Language proficiency
- Emergency contact Information
- Employer
- School
- Highest level of education
- Library card number
- Amount of fines waived

**How is information collected?**

Information is collected through a variety of different sources.

*Online Volunteer Application* - All ongoing SJPL volunteers create a profile in Better Impact, the volunteer management software SJPL uses to track volunteer applications, hours, and impact.
### Option 1
- Department Overview
- Information Collected: *Detailed analysis of all interactions with patron information*
- ALA Checklist Items
- Action Plan

### Option 2
- Department Overview
- What information is collected?
- How is the information collected?
- Who is the information shared with?
- Where is the information stored?
- How long is the information stored?
What’s Next?

“...I can only show you the door. You're the one that has to walk through it.” Morpheus, *The Matrix*

@mohawklibrarian  @juliedecimal  @PRIVACYALA  #chooseprivacy  Choose Privacy Week  (May 1 - 7, 2018)
1. Integration
2. Regular Checkups
3. Privacy Champion
4. Staff Training
OOH YEAH! CAN DO!

Questions?

Erin Berman (erin.berman@sjlibrary.org)
Julie Oborny (julie.oborny@sjlibrary.org)