DATA LIFECYCLES

Libraries promote themselves to users as havens from data collection and analysis. However, user data is everywhere and with it comes a multitude of opportunities for it to be compromised. It is overwhelming to consider all the different types of systems, policies, and procedures relating to user data. This often prevents libraries from addressing data privacy risks. You can mitigate that overwhelming feeling by understanding the data lifecycles in your library. Seeing how user data travels through the library will empower you to create policies and procedures that put user privacy first.

Data, Privacy, and the Library

User data collected by libraries can be divided into two types of Personally Identifiable Information (PII): data about you, and data that is linked to you.

PII 1 - DATA ABOUT A USER

- Name
- Physical/email address
- Date of birth
- User record number
- Library barcode
- Demographic information, including grade, year, major, and department

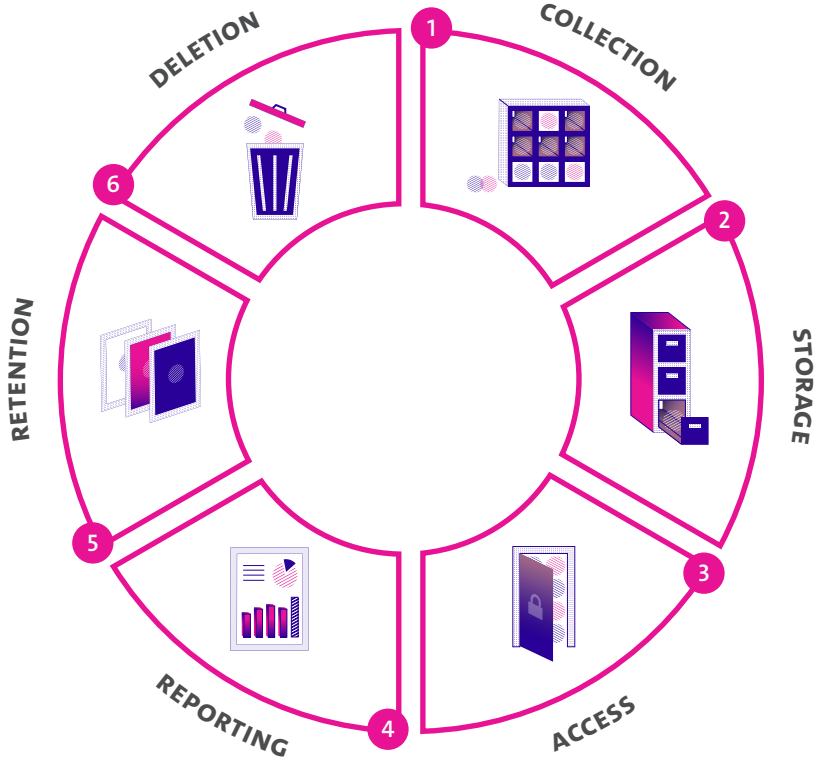
PII 2 - A USER'S ACTIVITIES

- Search & circulation histories
- Computer/wifi sessions
- Email and chat transcripts
- IP address; type of operating system or browser (digital fingerprint)
- eResource access
- Program attendance

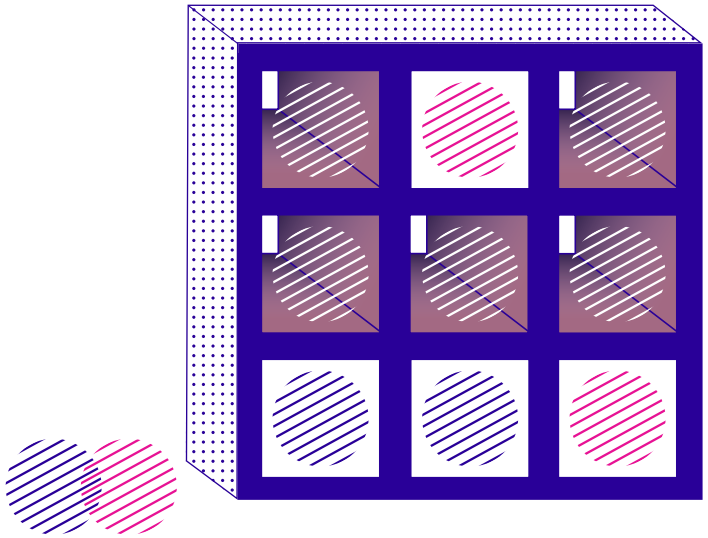
Each category contains data that can identify a real world individual. You can identify a person just by their activities; researchers have been able to identify individuals from data sets that only contain their search queries.

Library User Data Lifecycle

The library user data lifecycle helps to break down how user data is handled. It can also tell you how you might be putting your users' privacy at risk. There are six stages in the cycle: collection, storage, access, reporting, retention, and deletion.



Collection



Collection is one of the most crucial stages in terms of protecting user privacy. It is where you figure out what is collected as an institution and why it is collected. **Data that is not collected cannot be leaked or breached.**

|| **TIP** || Turn off settings that collect or store user data that the library does not need.

EXERCISE

What user data is collected at your library? The following list includes some common places user data is collected. Where else are you collecting user data at your library?

- Integrated library system
- Computer reservation system
- Library instruction data
- Data analytics software
- Your work email account
- Reference or information desk chat logs
- _____
- _____
- _____
- _____
- _____
- _____

EXERCISE

Data FOMO [Fear of Missing Out] is a thing! User data should only be collected if it has a specific operational need.

Review a user record to determine why data is being collected. Choose one piece of PII from the record and ask a co-worker (or yourself) why it's being collected. After asking, "Why?" the first time, ask it again. Do this five times or until you can no longer answer why.

DATA POINT FROM USER RECORD

- **Why is this information collected?**

_____

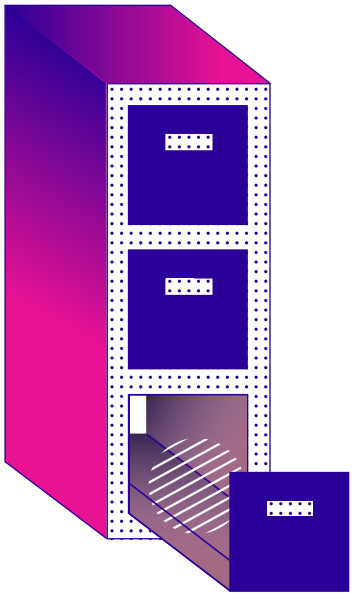
Why? _____

Why? _____

Why? _____

Why? _____

2 Storage



This stage covers physical and electronic storage at the library, in the cloud, or with a vendor. When thinking about where user data are stored, consider if multiple versions of the data are living in various places. The same data sets could be on backups, multiple desktops, email, or even a printout on someone's desk. Libraries should also consider what data sets that are stored in the same place could be combined to identify users. This is especially pertinent when raw (unmodified) user data from different systems is combined into one place, such as a data warehouse or data analytics application.

EXERCISE

Scavenger Hunt!

User data should be stored in the least number of places possible. Having multiple copies spread out in various locations increases the risk the data will be exposed or breached. Think of a type of user data collected at your library and go searching for all of the locations it might be found. For each location determine if the data is stored securely. This might be a locked cabinet or password protected file.

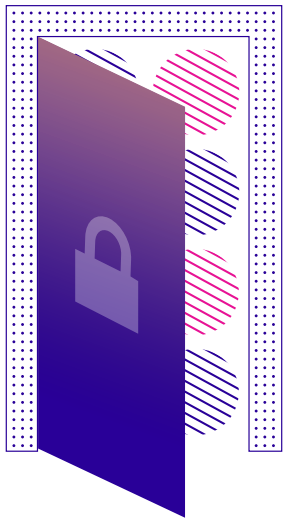
- What user data did you find?
- Does this data need to be stored in multiple locations?

DATA LOCATION	SECURED (Y/N)	HOW IS IT SECURED? HOW WILL YOU SECURE IT?

For items containing user data that are not secured consider the following:

- Store paper documents in locked desks or cabinets when not in use.
- Require individual user logins on all computers.
- Place electronic equipment in a space that has controlled entry (e.g. locked room or storage area).
- Require logins for public-facing staff computers and mobile equipment, including multifactor authentication, if possible.

3 Access



Physical access includes access to servers, computers, mobile devices, paper documents, and the spaces that contain all of those physical items. Electronic access includes user access levels in various systems and applications for both staff and vendors. Physical items that contain or have access to user data should be secured in locked areas and use passwords. For digital files, practice the "principle of least privilege," providing staff access to the least amount of user data that is necessary to perform specific tasks.

EXERCISE

Perform a self-evaluation to determine if you have the appropriate level of access to a library application or system that handles user data. Remember, everyone should be restricted to the lowest level of user data absolutely necessary for one to do their job. Some examples include integrated library systems, vendor products, social media accounts, Google Drive folders, etc.

APPLICATION OR SYSTEM	ACCESS LEVEL (CORRECT, SHOULD BE LOWER, SHOULD BE HIGHER)

*If you are a supervisor or someone at your library with control over staff accounts, perform this same evaluation for all applications or systems to determine if each individual has the appropriate access levels.

Perform an annual audit of access levels for staff for both electronic and physical access to user data. Use the Privacy Audit Field Guide for assistance in this process.

- Deactivate accounts of staff no longer working at the library.
- Change user permissions for staff who changed positions or gained/lost job responsibilities.
- Look at which vendors have user accounts and if they still need access to the system.

4 Reporting

Reporting user data can take many forms, from internal dashboards for staff (such as checkouts and gate counts) to publishing library data as Open Data. Libraries should be cautious in how and what data they report as it can be a way to inadvertently share a user's PII.

WHAT TO WATCH OUT FOR

Giving access to unmodified user data to all staff.

Publishing raw user data to public sources.

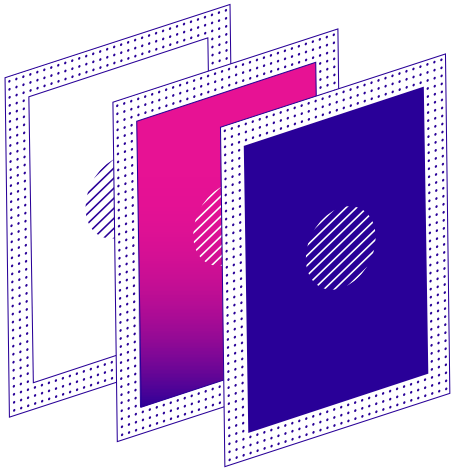
Sharing of user data with marketers and resellers, including user data collected by vendors.

Being a "good citizen" while helping with law enforcement requests - giving more information than requested under a warrant or subpoena, or even giving information to law enforcement without one.

HOW TO PROTECT USER PRIVACY

- Offer aggregated data through dashboards and canned reports.
- Create policies and procedures surrounding publishing data to external audiences, including privacy risk audits of data sets marked for publication.
- School and academic libraries should consult with legal counsel around the Family Educational Rights and Privacy Act (FERPA) educational record disclosure policies.
- Does the library have a law enforcement request procedure? If not, or if the policy has not been updated for a while, here are a few resources from ALA to start the process:
  - How to Respond to Law Enforcement Requests for Library Records and User Information: Suggested Guidelines (http://bit.ly/lawresponse)
  - Law Enforcement Inquiries (http://bit.ly/lawinquire)

5 Retention



How long the library keeps user data depends on several factors, including legal regulations and operational considerations. Every library should have a retention policy. Your local governing body (school, city, county) may already have a retention policy that you can follow. There are very few items containing user data that should be kept forever! Make sure to check local and state regulations too. Some data may be exempt from retention regulations.

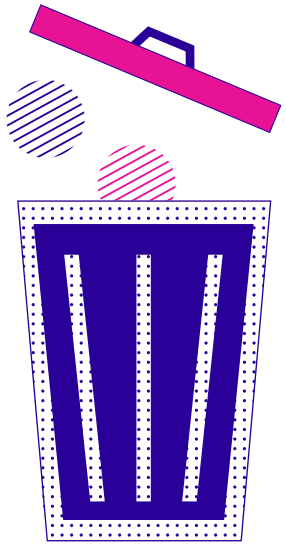
A library consortium should have retention policies and procedures for its member libraries to ensure the same level of user privacy throughout the consortium.

EXERCISE

Create a record retention schedule for library data, including user data, system backups, and logs. Ensure that it is in compliance with local and state regulations.

DATA	FORMAT	WHAT DATA IS RECORDED?	WHERE IS IT LOCATED?	WHO HAS ACCESS?	HOW LONG IS THE DATA KEPT?
Library card application	*Paper* *Electronic*	*Name* *Date of birth* *Address* *Email* *Telephone*	*Circulation desk* *ILS server*	*All staff with ILS access*	*Paper applications are shredded after one week.* *Digital applications are purged every 30 days.*

6 Deletion



Deletion of data includes the disposal of electronic and physical media, as well as electronic files. Once a data point is collected, it is very hard to delete it from existence. User data can even be exposed by not properly disposing of electronic equipment. There have been cases where sensitive information has been pulled from discarded copy machine's hard drives! Along with proper electronic equipment disposal, make shredding a regular part of your library's healthy privacy practices. Any paper that includes a user's PII (including email) should be shredded.

EXERCISE

Have a shredding party! Schedule a time for staff to bring paper documents containing user data to shred at their location (staff should not travel with documents containing PII). If the library does not have access to a shredder, there are companies that will shred for a fee.

Hard drives or disks no longer in use should be destroyed. If there are plans to reuse a drive that contained user data, ask the IT department to help wipe it before use.

NOTES

ALA American Library Association

PRIVACY ADVOCACY GUIDES

Privacy is a core value of librarianship, yet it often feels like an overwhelming and onerous undertaking. Use these Privacy Field Guides to start addressing privacy issues at your library. Each guide provides hands-on exercises for libraries. Check out all the available guides at **bit.ly/PrivacyFieldGuides.**

INSTITUTE of Museum and Library SERVICES

This project was made possible in part by the Institute of Museum and Library Services LG-36-19-0073-19.

Designed by PixelbyInch.com