Library Privacy and Vendor Management II: Exploring Practical Strategies and Best Practices

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

May 2020

Pacific Library Partnership

INSTITUTE *of* **Museum** and **Library** SERVICES

LDH Consulting Services

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
CalOPPA	California Online Privacy Protection Act of 2003
CCPA	California Consumer Privacy Act
COPPA	Children's Online Privacy Protection Act
FERPA	Family Educational Rights and Privacy Act
GDPR	General Data Protection Regulation
IANAL	I Am Not A Lawyer (always a good acronym to have in your back pocket!)
ISO	International Organization for Standardization
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
PII	Personally Identifiable Information
RFI	Request For Information
RFP	Request For Proposals

Patron Data Lifecycle
Quick Reference Map

Phase	Question	Best Practice
Collection	What patron data are you collecting, and why?	Only collect data needed for demonstrated business cases Practice "The Five Whys"
Storage	Where is the patron data stored?	Limit number of data storage areas Limit storage of patron data in local and vendor systems
Access	Who has access to the paton data?	Limit physical and electronic access to data Audit vendor security and privacy practices
Reporting	What patron data is published to staff and to the public?	Aggregate data and control access to data through dashboards, database views, and other data reporting tools
Retention	How long is patron data kept?	Follow local and state retention regulations Ensure backups and logs are covered in retention policies
Deletion	How is patron data deleted?	Properly dispose of physical and electronic media that contained patron PII

Vendor Relationship Lifecycle
Quick Reference Map

Phase	Best Practices and Tools

Selection

Use Request for Information (RFI) to gather information about general vendor privacy practices

Include data privacy and security Functional Requirements in Request for Proposals (RFPs)

Onboarding

Plan strategies and identify compromise and dealbreaker items before starting contract negotiations

Use contract addendums and non-disclosure agreements (NDAs)

Maintaining

Schedule and conduct regular security and privacy audits

Review impact on patron privacy of major changes in contract or product functionality and choose to either renegotiate the contract or non-renewal

Separation

Work with vendor to export and delete patron data when the business relationship ends

Exercises

Exercise – RFP Show & Tell

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

What does your RFP section cover with regard to privacy?

What is the main strength of your RFP section?

What is one way your RFP section can be improved in protecting patron privacy?

Exercise – Contract Flags

Every contract will include at least one flag, and there are many flags to watch out for. Here is a small list of important contract flags to look for when reading the contract with a privacy lens:

- "Reasonable" and use of other vague terms to describe privacy or security practices
- Lack of definitions for terms
- Termination of contract – no information about what happens to your library's data after the business relationship ends
- Data ownership
- Lack of information about responses to law enforcement or government data requests

- Legal jurisdiction of the contract
- Lack of transparency in contract details
- Indemnity/liability clauses
- Data reselling or disclosure to other third parties
- Monitoring patron use (including web analytics)
- Using "Aggregated", "Anonymized", "De-identified" without defining methods

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

What red flags in the above list did you identify in the contract?

Were there any red flags not on the list that you found in the contract? If so, what were they and why would you consider them red flags?

Have you encountered these red flags at your library? If so, how did you address them with the vendor?

Library Privacy and Vendor Management II: Exploring Practical Strategies and Best Practices

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

INSTITUTE *of* **Museum** and **Library** SERVICES

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.

Workshop Housekeeping - Logistics
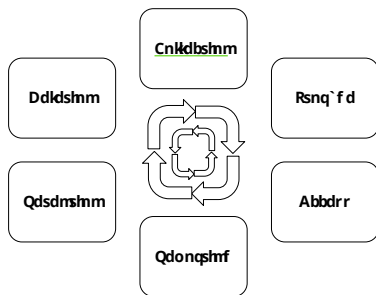
IANAL; Consult legal staff for legal advice

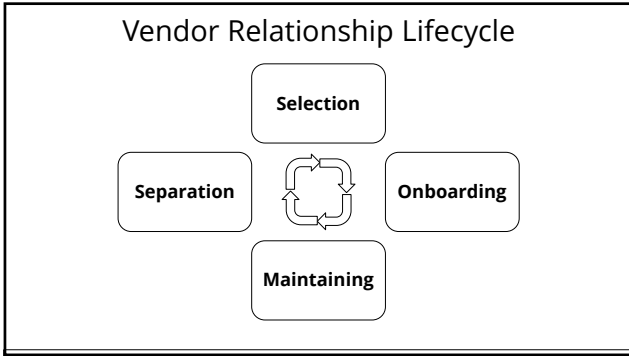Exercises and Discussions - what to expect

Toolkit tie-in

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

---

Section One:
Refresher on Vendors and Libraries

Library Patron Data Lifecycle

Cnkkdbshnm

Ddkdshnm

Rsnq`f d

Qdsdmshnm

Abbdrr

Qdonqshmf

Vendor Relationship Lifecycle

- Selection
- Onboarding
- Maintaining
- Separation

Section Two:
Selection Best Practices and Strategies

Selection - Where to start?

RFI - Request for Information

Used to gather information about services or products

Potential uses:

- Obtain privacy policies
- Gather information about <u>general</u> privacy features

RFP - Request for Proposals

Used to gather bids from potential vendors

Potential uses:

- Outline privacy reqs
- Gather information about <u>specific</u> privacy features

Exercise –
RFP Show & Tell

Section Three:
Onboarding – ALL the Contracts

Contracts and Legal Regulations

- California Gov Code § 6267
- California Consumer Privacy Act of 2018 (CCPA)
- California Civil Code Section 1798.82
- Family Educational Rights and Privacy Act (FERPA)
- Children's Online Privacy Protection Act (COPPA)
- Local Regulations, including record retention schedules and public disclosure exemptions and regulations
- Parent institution policies or contract boilerplate

Onboarding – Privacy & Contract Red Flags

- "Reasonable" and vague terms
- Lack of definitions for terms
- Indemnity/liability clauses
- Termination details – data exit
- Lack of information about responses to law enforcement or government data requests
- Legal jurisdiction!
- Lack of transparency
- Data ownership
- Data reselling or disclosure to other third parties
- Monitoring patron use (web analytics)
- Using "Aggregated", "Anonymized", "De-identified" without defining methods

Exercise – Contract Flags

Onboarding - Contract Addendum and NDA

Contract Addendum

- Legal boilerplate for standard privacy and security contract language
- Can be used in both initial contract signings and renewal periods

Non Disclosure Agreement

- AKA NDAs
- Limit or prohibit sharing of patron data to:
  - Subcontractors
  - Service Providers
  - Other Third Parties

Walkthrough – Contract Addendum

_____

_____

_____

_____

_____

_____

Section 3.5 Communications

_____

_____

_____

_____

_____

_____

Onboarding – Communications

Staff
- Announcements via:
  - Email
  - Staff Intranet
  - Meetings
- Vendor privacy notice list
- Update privacy policies if necessary

Patrons
- Press releases or news announcements
- Vendor privacy notice list on public site
- Update privacy notice if necessary

_____

_____

_____

_____

_____

_____

Discussion –
Public Communication
Examples

Section Four:
Maintenance Best Practices and
Strategies

Walkthrough –
Vendor Audit

Section Five:
Wrap up

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

Thank you

:-)

LDH
Consulting
Services

Becky Yoose
Library Data Privacy Consultant
LDH Consulting Services

Email:
becky@ldhconsultingservices.com

References and Further Reading

General

Ayre, Lori Bowen. 2017. "Protecting Patron Privacy: Vendors, Libraries, and Patrons Each Have a Role to Play." Collaborative Librarianship. March 2017. Access September 6, 2019. https://digitalcommons.du.edu/cgi/viewcontent.cgi?article=1330&context=collaborativelibrarianship.

Bettilyon, Tyler Elliot. 2019. "Why 'Anonymized Data' Isn't So Anonymous." OneZero. April 24, 2019. https://onezero.medium.com/why-anonymized-data-isn-t-so-anonymous-535d2db75a2d.

Breeding, Marshall. 2015. "Privacy and Security of Automation and Discovery Products." Accessed September 6, 2019. https://librarytechnology.org/repository/item.pl?id=20425.

Garfinkel, Simson L. 2015. "De-Identification of Personal Information." *NIST Interagency/Internal Report (NISTIR) - 8053*, October. https://www.nist.gov/publications/de-identification-personal-information.

Green, Ben Z., Gabe Cunningham, Ariel Ekblaw, Andrew Linzer, Paul M. Kominers, and Susan Patricia Crawford. 2017. "Open Data Privacy." https://dash.harvard.edu/handle/1/30340010.

Grub, Tammy. 2016. "Chapel Hill hopes portal is key to more knowledge, understanding." Raleigh News & Observer. Accessed September 13, 2019. https://www.newsobserver.com/news/local/community/chapel-hill-news/article87795422.html.

Halaychik, Corey S. 2015. "Finding a Way: Library Master Agreements at the University of Tennessee." *Journal of Electronic Resources Librarianship* 27 (3): 171–81. https://doi.org/10.1080/1941126X.2015.1059644.

Hess, Stephanie, Megan Kilb, and Iris Garcia. 2020. "Contract Construction: Creating an Effective Licensing Toolkit in an Academic Library Setting." *The Serials Librarian* 0 (0): 1–6. https://doi.org/10.1080/0361526X.2020.1707021.

Hill, Kate, and Tessa Minchew. 2018. "Into the Great Wide Open: Licensing, Vendor Relations, and Data Security During 'Interesting Times'." Electronic Resources & Libraries 2018. Accessed September 6, 2019. https://www.dropbox.com/sh/r8yfxwl7h602au6/AABGaKVbMbEg7AnmijmTOApda?dl=0&preview=S079+-+Into+the+Great+Wide+Open+(1).pptx.

Kelly, Robert G. 2013. "Biz of Acq -- Negotiating with a Contract Addendum." Against the Grain 20 (3). https://doi.org/10.7771/2380-176X.2412.

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.

Kritikos, Katie, and Michael Zimmer. 2017. "Privacy Policies and Practices with Cloud-Based Services in Public Libraries: An Exploratory Case of BiblioCommons." Journal of Intellectual Freedom and Privacy 2 (July): 23. https://doi.org/10.5860/jifp.v2i1.6252.

Lambert, April D., Michelle Parker, and Masooda N. Bashir. 2015. "Library patron privacy in jeopardy: An analysis of the privacy policies of digital content vendors." Proceedings of the Association for Information Science and Technology. 2015. Accessed September 6, 2019. https://doi.org/10.1002/pra2.2015.145052010044.

"LIBLICENSE." Accessed March 4, 2020. http://liblicense.crl.edu/.

Magi, Trina J. 2010. "A content analysis of library vendor privacy policies: Do they meet our standards?" University Libraries Faculty and Staff Publications. Accessed September 6, 2019. https://scholarworks.uvm.edu/libfacpub/5.

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

"New Future of Privacy Forum Study Finds the City of Seattle's Open Data Program a National Leader in Privacy Program Management." n.d. Accessed April 10, 2018. https://fpf.org/2018/01/25/new-future-of-privacy-forum-study-finds-the-city-of-seattles-open-data-program-a-national-leader-in-privacy-program-management/.

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

"NISO Consensus Principles on User's Digital Privacy in Library, Publisher, and
Software-Provider Systems (NISO Privacy Principles)." National Information
Standards Organization. December 10, 2015. Accessed September 6, 2019.
https://www.niso.org/publications/privacy-principles.

"Privacy with Google Analytics | Field Reports." 2018. Library Journal. March 19, 2018.
https://lj.libraryjournal.com/2018/03/lj-in-print/privacy-google-analytics-field-
reports/.

Rodriguez, Michael. 2017. "Wrangling Services Contracts in Libraries." In *Roll With the
Times, or the Times Roll Over You*. Purdue University Press.
https://doi.org/10.5703/1288284316487.

Rodriguez, Michael, Jason Chabak, Lindsay Cronk, Allen Jones, Christine Stamison, and
Kimberly Steinle. 2018. "Managing Vendor Relationships." *Charleston Library
Conference*, October 2018.
https://docs.lib.purdue.edu/charleston/2018/management/6.

SBS CyberSecurity. 2019. "What Documentation Should You Review for a Critical
Vendor?" https://sbscyber.com/resources/what-documentation-should-you-
review-for-a-critical-vendor.

Smith, Jane, and Eric Hartnett. 2015. "The Licensing Lifecycle: From Negotiation to
Compliance." *The Serials Librarian* 68 (1–4): 205–14.
https://doi.org/10.1080/0361526X.2015.1017707.

Yoose, Becky. 2018. "Data Analytics and Patron Privacy in Libraries: A Balancing Act."
Accessed April 8, 2018. https://2018.code4lib.org/talks/data-analytics-and-patron-
privacy-in-libraries-a-balancing-act.

Zimmer, Michael. 2013. "Assessing the Treatment of Patron Privacy in Library 2.0
Literature." Information Technology and Libraries. Accessed September 6, 2019.
https://doi.org/10.6017/ital.v32i2.3420.

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." Text. Advocacy, Legislation & Issues. July 7, 2006. http://www.ala.org/advocacy/intfreedom/statementspols/otherpolicies/policyconcerning.

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

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

———. 2014. "Questions and Answers on Privacy and Confidentiality" Advocacy, Legislation & Issues. Accessed April 8, 2018. http://www.ala.org/advocacy/privacy/FAQ.

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

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

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

California Law Resources

"California Civil Code § 1798 Title 1.81 Customer Records." Accessed January 31, 2020. http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.&part=4.&chapter=&article=.

"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=625
4.&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=626
7.&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/.

RFP and Contract Resources and Templates

ALA. 2019. "Implementing Library Technology: Request for Proposal (RFP) Writing."
Accessed September 6, 2019. https://libguides.ala.org/librarytech/rfp-writing.

EDUCAUSE. n.d. "Data Protection Contractual Language." Accessed March 4, 2020.
https://www.educause.edu/focus-areas-and-initiatives/policy-and-
security/cybersecurity-program/resources/information-security-
guide/toolkits/data-protection-contractual-language.

———. n.d.b. "Template Non-Disclosure and Confidentiality Agreements." Accessed
March 4, 2020. https://library.educause.edu/resources/2012/3/template-
nondisclosure-and-confidentiality-agreements.

NYC Department of Education. 2014. "RFP Information Security Requirements."
Accessed September 6, 2019.
https://forallschools.s3.amazonaws.com/static/images/forallrubrics-

home/DOE%20RFP%20Information%20Security%20Requirements%2007-02-2014%20(Final).pdf.

Wilkinson, Frances, and Sever Bordeianu, eds. 2018. The Complete Guide to RFPs for Libraries. Libraries Unlimited. http://publisher.abc-clio.com/9781440859403.

Negotiation Resources

Berdzeni, Natalya. 2016. "Negotiation tips for library directors." LAC Group. February 22 2016. Accessed September 6, 2019. https://lac-group.com/negotiation-tips-library-professionals/.

Boss, Richard W. n.d. "Negotiating Contracts with Integrated Library System Vendors." PLA Tech Notes. https://alair.ala.org/bitstream/handle/11213/258/Negotiating%20with%20ILS%20Vendors.pdf?sequence=99&isAllowed=y.

Dygert, Claire T., and Elizabeth Parang. 2013. "Honing Your Negotiation Skills." The Serials Librarian 64 (1–4): 105–10. https://doi.org/10.1080/0361526X.2013.760395.

Gruenberg, Michael. 2015. "Both Sides Now: Vendors and Librarians - Managing the Negotiation Process with Library Vendors." Against the Grain. Accessed September 6, 2019. https://www.against-the-grain.com/wp-content/uploads/2015/03/both_sides_now_v26-6.pdf.

Marsh, P. D. V. 2001. Contract Negotiation Handbook. Gower Publishing, Ltd.

Stroshane, Eric. 2017. "Negotiating Contracts with Vendors for Privacy." Intellectual Freedom Blog. May 3, 2017. Accessed September 6, 2019. https://www.oif.ala.org/oif/?p=9578.

Examples

Contract Addendums

Marmot Library Network. 2016. "Confidentiality, Privacy, and Security Addendum." Accessed February 15, 2020. https://www.marmot.org/sites/default/files/Privacy%20Addendum%20Marmot%20MCVSD51.pdf.

Request For Proposals (from the RFP exercise)

Chicago Public Library. 2015. "Request for Proposal ('RFP') for Library Management System." https://librarytechnology.org/docs/librfp-8-main.pdf.

New York City Department of Education. 2014. "RFP Information Security Requirements." https://forallschools.s3.amazonaws.com/static/images/forallrubrics-home/DOE%20RFP%20Information%20Security%20Requirements%2007-02-2014%20(Final).pdf.

Orbis Cascade Alliance. 2012. "Request for Proposal Shared Library Management Service." https://www.odin.nodak.edu/sites/default/files/rfp_shared_library_management_service_final.pdf.

SUNY. 2017. "Request for Proposal #CM03130 Library Services Platform." https://librarytechnology.org/docs/librfp-123-main.pdf.

Vendor Assessment Tools

Caro, Alex and Chris Markman. 2016. "Measuring Library Vendor Cyber Security: Seven Easy Questions Every Librarian Can Ask." The Code4Lib Journal. Accessed June 13, 2019. https://journal.code4lib.org/articles/11413.

EDUCAUSE. n.d. "Higher Education Community Vendor Assessment Toolkit." Accessed March 4, 2020. https://library.educause.edu/resources/2016/10/higher-education-community-vendor-assessment-toolkit.

Information Security Office. n.d. "Details of the Vendor Security Assessment Program." University of California Berkeley. Accessed February 26, 2020. https://security.berkeley.edu/services/vendor-security-assessment-program/details-vendor-security-assessment-program.

Quintin, Cooper, and Soraya Okuda. 2018. "How to Assess a Vendor's Data Security." Electronic Freedom Foundation. January 8, 2018. Accessed September 6, 2019. https://www.eff.org/deeplinks/2018/01/how-assess-vendors-data-security.

"SJPL Vendor Security Analysis" n.d. Accessed June 13, 2019. https://drive.google.com/drive/folders/1jdPwQeC5RAUbBWLAhyIYxWHa0pTdVObc

"Vendor Security Assessment Questionnaire." Santa Cruz Public Library. Accessed January 13, 2020. https://www.santacruzpl.org/files/data_privacy/docs/SCPLVendorSecurityAssessmentQuestions.pdf.