Chapter 4

Third-Party Platforms

Many libraries rely to some degree on applications hosted outside the library's direct administrative control or ownership, such as library services platforms, applications hosting and provisioning content (electronic journal publishers, e-book content providers, etc.), analytics tools, social media platforms, and more. Many services offer personalization features or other unique account-based services allowing end users to tailor their experience. Some services collect data that by itself could be considered private information; the potential also exists that data streams from one application could be combined with data from another application to create a more detailed profile of the user. In today's increasingly distributed environment, the library can no longer be considered the sole gatekeeper of its patrons' private information, emphasizing the present reality that data privacy can be confusing, ambiguous, and opaque.

ALA's Privacy Tool Kit and associated work demonstrate sound recognition of how distributed and complex today's online library environment has become. ALA's *Resolution on the Retention of Library Usage Records* urges, among other things, that libraries "assure that vendor agreements guarantee library control of all data and records."[1] The Tool Kit's "Developing or Revising a Library Privacy Policy" notes, "When developing and revising policies, librarians need to ensure that they limit the degree to which the library and third party service providers monitor, collect, disclose, and distribute personally identifiable information."[2] Related to privacy concerns with emerging technologies, it notes, "The lack of transparency in consent, data sharing and terms of service changes is a barrier to patron-centered service; it's imperative that libraries understand each new technology by defining them and identifying the mechanism through which each patron's privacy may be breached."[3] It further notes concerns with various types of applications and hosting models that have increasingly become the norm, such as apps, cloud computing, OPACs, and social networking tools.

ALA's "Privacy and Confidentiality Q&A" notes several related questions, for example,

> 22. Does the library's responsibility for user privacy and confidentiality extend to licenses and agreements with outside vendors and contractors?
>
> Most libraries conduct business with a variety of vendors in order to provide access to electronic resources, to acquire and run their automated systems, and in some instances, to offer remote storage (e.g. "cloud computing") or to enable access to the Internet. Libraries need to ensure that contracts and licenses reflect their policies and legal obligations concerning user privacy and confidentiality. Whenever a third party has access to personally identifiable information (PII), the agreements need to address appropriate restrictions on the use, aggregation, dissemination, and sale of that information, particularly information about minors. In circumstances in which there is a risk that PII may be disclosed, the library should warn its users.[4]

Similarly, *Privacy: An Interpretation of the Library Bill of Rights* notes,

> Libraries should never share users' personally identifiable information with third parties or vendors that provide resources and library services, unless the library obtains explicit permission from the user or if required by law or existing contract. Libraries or their governing institutions should negotiate agreements with vendors that retain library ownership of user data and permit independent auditing of vendor data collection, retention,

> and access policies and practices. Such agreements should stipulate that user data is confidential and that it may not be used or shared except with the permission of the library.[5]

As noted in chapter 1, ALA's Intellectual Freedom Committee has created several privacy checklists, many of which can apply to third-party vendor relationships where the application, service, or content is hosted outside the library's direct control and possession. These checklists provide guidance on recommended data stewardship related to vendors and steps the library can take to better inform its patrons about third-party privacy considerations and practices. As just one example, the "Library Privacy Checklist for E-Book Lending and Digital Content Vendors" notes,

> Provide links to vendor privacy policies and terms of service pages for users when appropriate, e.g. from the library's own privacy policy page or from a library web page about the vendor's product or service.
>
> Work with vendors to configure services to use the opt-in method whenever possible for features that involve the collection of personal information.
>
> . . .
>
> Add privacy considerations to the library's selection criteria for new purchases or the renewal of existing purchases.[6]

ALA's "Library Privacy Guidelines for Vendors" notes,

> Libraries and vendors must work together to ensure that the contracts and licenses governing the collection, processing, disclosure, and retention of library user data reflect library ethics, policies, and legal obligations concerning user privacy and confidentiality.
>
> . . .
>
> **Agreements, Ownership of User Data, and Legal Requirements**
>
> Agreements between libraries and vendors should address appropriate restrictions on the use, aggregation, retention, and disclosure of user data, particularly information about minors. Agreements between libraries and vendors should also specify that libraries retain ownership of all user data and that the vendor agrees to observe the library's privacy policies and data retention and security policies.
>
> . . .
>
> Privacy policies should be made readily accessible and understandable to users. Safeguarding user privacy requires that individuals know what information is gathered about them, how long it is stored, who has access to it and under what conditions, and how it is used. There should be a way to actively notify ongoing users of any changes to the vendor's privacy policies.
>
> . . .
>
> **Company Sale, Merger, or Bankruptcy:** In the event that a vendor is sold to another company, merges with another company, or is dissolved through bankruptcy, all personally identifiable information should be held under the same privacy policy or securely destroyed. Libraries and their users should be notified and provided a method to request that their data be securely destroyed or exported.[7]

In the library privacy policies examined, applications housed outside the libraries' direct administrative control were indeed often called "third-party" providers or websites; this occurred in seventeen of the academic library and fourteen of the public library policies analyzed. An additional ten libraries referred to such services but without the specific moniker "third-party." Other terminology used included "internet sites and services outside the administrative domain"[8] and "other sites and services that are not contained nor controlled within the Library's online environment."[9] This chapter will focus on several important considerations related to third parties, including how libraries typically do not share private patron information outside the library, how libraries working with vendors encourage them to adhere to the library's privacy practices, and how notices encourage patrons to review the policies of third-party vendors.

Sharing of Private Information

Many library policies explicitly indicate the libraries do not share customer information with outside entities (which could be third-party providers or other third parties that do not provide services or content to the library). Several verbs are used across the policies to denote that the library does not share information, including *sell, lend, license, disclose, provide, lease, rent, release, share, give, transfer, trade,* and *provide access*. Several policies indicate more generally that the library keeps information confidential and access is not provided for commercial use. At least half of the public library policies analyzed and fifteen of the academic library policies made specific reference to how they do not share confidential information with third parties. As with other analysis points in this study, the fact that some policies don't specifically address the sharing of information with outside entities does not imply or suggest that the library does sell information to outside entities—only that sharing of information wasn't specifically referenced in the policy. For example, numerous policies indicate that confidential information will be released only by court order, and so on, and this implies that the library does not, for example, sell information for commercial use, even if the explicit reference does not appear. Several policies specifically note that their state's law explicitly prohibits any practice of selling information, such as Beaufort County Library's policy, which states, "Under Title 60-4-10 of the South Carolina Code of Laws, the Library may not sell, trade or rent its customers' personal information."[10] Examples of library policy phrasing stating that the library does not sell, lease, and so on confidential information follow.

East Greenbush Community Library

> The Library does not sell, lease, or otherwise distribute or disclose patron name, email address, postal address, telephone number, or other personal information to outside parties.[11]

Musser Public Library

> The library will hold confidential the names of card holders and their registration information, including email addresses, and not provide access for private, public or commercial use.[12]

Genesee District Library

> All gifts, grants, and/or support must ensure the confidentiality of user records. The library will not sell or provide access to library records in exchange for gifts or support.[13]

Phoenix Public Library

> Phoenix Public Library does not sell, rent, lease, or otherwise provide its customer lists or customer-controlled information to third parties.[14]

Cornell University Library

> The Library will not sell, share, or otherwise distribute your personal data to third parties without your consent.
>
> . . .
>
> The Library expects the information service providers with whom we contract to protect the identity of individual users and the information they use. We commonly require, for example, that vendors agree not to sell or license information from library users to third parties.[15]

Montana State University Library

> If you consent to give us your personally identifiable information, we will keep it confidential and will not sell, license, or disclose personal information to any third party without your consent, unless we are compelled to do so under the law or to comply with a court order.
>
> . . .
>
> Third Party Security: We ensure that our library's contracts, licenses, and off-site computer service arrangements reflect our policies and legal obligations concerning user privacy and confidentiality. Should a third party require access to our users' personally identifiable information, our agreements address appropriate restrictions on the use, aggregation, dissemination, and sale of that information.[16]

Cornell University Library's document "Library Practices on the Collection, Use, Disclosure, Maintenance and Protection of Personally-Identifiable Information" has a section titled "Licensed Service Case Study: The Library Catalog," wherein the library describes its use of OCLC's services for its library catalog, references OCLC's service terms and conditions, and provides some analysis of the types of information collected as well as the fact that "individual users are not connected to activities performed on the site. . . . Searches conducted and records viewed cannot be tied back to individual users."[17]

Working with Vendors to Respect Library Privacy Policies and Values

Several professional organizational statements or frameworks have been developed to encourage vendor respect for library privacy practices. The International Coalition of Library Consortia's *Privacy Guidelines for Electronic Resources Vendors* advocates that vendors draft transparent and accessible privacy policies that empower and protect end users and seeks adherence to the ALA *Code of Ethics*.[18] Harvard Library's privacy policy references this document: "Our commitment to user privacy extends to our agreements with online content providers, including support for the International Coalition of Library

Consortia (ICOLC) Privacy Guidelines for Electronic Resources Vendors."[19]

Stanford Libraries' "Statement on Patron Privacy and Database Access" states that providers increasingly have data-gathering practices in conflict with a library patron's right to privacy and notes, "It is important for libraries to monitor these developments and redirect them in favor of patron privacy in order to safeguard our role as trusted providers in the information age."[20] Duke University Library's privacy policy references the Stanford Libraries' statement: "DUL additionally endorses the Stanford Libraries Statement on Patron Privacy and Database Access."[21]

Approximately fifteen academic library and three public library policies provided some reference noting their libraries' efforts seeking to ensure that commercial vendors adhere to the local library's privacy stance.

Encouraging Patrons to Review the Policies of Third-Party Vendors

Approximately twenty-seven of the academic library and twenty-four of the public library policies make some reference to third-party privacy policies and the ways those vendor policies apply when patrons are using that site or service, encouraging patrons to read the privacy policies of third-party vendors. Phrasing varies broadly, but a core, cautionary, and underlying message is that providers have their own policies, that the patron is subject to those policies, and that third parties may not value patrons' privacy to the same degree as the library.

Brown County Library

> The Library does not collect information about who library users are, but other organizations might. The Library encourages library users to become familiar with the privacy policies of their ISP (Internet Service Provider) and the websites that they visit to learn what information might be collected elsewhere online.
>
> . . .
>
> The Library's website contains links to other sites. The Brown County Library is not responsible for the privacy practices of other sites, including providers of online database services for which the Library subscribes, which may be different from the privacy practices described in this policy. The Library encourages library users to become familiar with privacy policies of other sites visited, including linked sites.[22]

Nashville Public Library

> You are agreeing to be bound by these terms, all applicable laws and regulations, and any other applicable policies, terms and guidelines established by NPL and those of any third parties that host our sites (such as Facebook or Twitter).[23]
>
> Nashville Public Library's website includes many links to outside sources. Those sites have different privacy statements and the Library's notice does not apply. Individuals should always take care before sharing personal information, credit card numbers, or other sensitive information via the Internet.[24]

Los Angeles Public Library

> Depending on the third-party tool's business practices, privacy policies, terms of service, and/or the privacy settings you selected, the information you have provided to third parties could be used to identify you when you visit lapl.org. These third parties do not/will not share your identity with lapl.org.
>
> . . .
>
> Non-library websites may be linked through the library's website. Many non-library sites may or may not be subject to the Public Records Act and may or may not be subject to other sections of California Code or federal law. Visitors to such sites are advised to check the privacy statements of such sites and to be cautious about providing personally identifiable information without a clear understanding of how the information will be used.[25]

Rutgers University Libraries

> Third Party Security: The Rutgers University Libraries use and link to resources owned and operated by third parties, including integrated library systems, offsite computer services, databases, and electronic journals. We license these resources for the use of Rutgers authorized users. We make every attempt to include user privacy protections in license agreements with third parties, such as vendors of digital information resources like electronic databases and journals. Nevertheless, because the use of these websites and resources is not governed by the Rutgers University Libraries, we strongly recommend that you review the privacy policies of the websites that you visit, particularly if you are requesting online help through email or chat or establishing your own account for

> specialized services like table of contents, email, saved search alerts, purchases, or personalization features. When connecting to licensed resources outside the library, we authenticate users as members of our community and do not provide any personally identifiable information.[26]

University of North Carolina at Chapel Hill Libraries

> **Vendors and Other Entities**
>
> On The University of North Carolina at Chapel Hill Libraries' behalf, vendors and other third parties may provide certain services available on the libraries' Web sites. The University of North Carolina at Chapel Hill Libraries may provide information, including personal information, collected on the Web to third-party service providers to help us deliver programs, products, information and services. Service providers are also an important means by which The University of North Carolina at Chapel Hill Libraries maintains its Web site and mailing lists. We will take reasonable steps to ensure that these third-party service providers are obligated to protect, de-identify, or dispose of personal information on our behalf.
>
> We license resources from vendors who may, in turn, request information from you for services, e.g., "notify me" or "alert" services. We encourage you to understand the privacy policies of those vendors and take personal responsibility for protecting your personal information.[27]

Utah State University Libraries

> USU Libraries website may contain links to other resources that are independently managed. The Library also contains links to sources outside the university. These sites may have their own privacy policy or may have none at all. We urge you to use caution when providing personal information to any of these websites.[28]

Cornell University Library

> More and more, the Library outsources systems and services to third-party vendors. Most of the digital resources that we offer, for example, come from outside suppliers, as does the current Library Catalog. The Library expects the information service providers with whom we contract to protect the identity of individual users and the information they use. We commonly require, for example, that vendors agree not to sell or license information from library users to third parties. Many vendors provide additional personalized services that may require you to identify yourself with your name or a pseudonym. In general, this is done at your discretion; the Library seeks to avoid products that demand personalization.
>
> While the Library seeks to require third parties with which it works to follow accepted library policies regarding privacy and confidentiality, it is not responsible for the privacy practices of these third parties. We encourage users to familiarize themselves with third party privacy policies before using the resources.[29]

Google Analytics

Google Analytics appeared to be the single most referenced third-party platform across the analyzed policies, mentioned by name in at least nine of the public and thirteen of the academic library policies, and its use seems implied in the policies of several additional libraries. Some policies go into greater detail about their use of Google Analytics, for example, the University of California Berkeley Library's policy:

> **Google Analytics**
>
> The UC Berkeley Library uses Google Analytics to capture and analyze web statistics. Google Analytics is a cookie-based analytics program that uses cookies to track website activity. Google Analytics typically collects, at least temporarily, the following information: Network Location; Hostname; web pages requested; referring web page; browser used; screen resolution; date and time. No personal information is stored within cookies. Cookies can be disabled within a browser's preference or option menu.
>
> For more information about Google Analytics, see Google Privacy Center—Privacy Policy.[30]

Several policies note that the user can curtail the information collected, for example, the University of Denver Libraries' policy:

> The Libraries' website (OmniUpdate), research guides (Springshare), A-Z database list, Special Collections @ DU, Archives @ DU (Archives Space), Digital Commons @ DU (Digital Commons), Compass (Primo), Online Exhibits (Omeka), and Yewno are tracked using Google Analytics. Data gathered include the browser, operating system, and city of the device being used, searches performed, and site navigation. The Libraries do not use Google Advertising Features, so no personal or demographic data are made available to the Libraries

> via Analytics. However, if you are logged into your Google Account while using the Libraries' website or tools, additional data may be tracked and linked to your Google Account.
>
> Additional information, including instructions on adjusting what data Google connects to your account, can be found at:
>
> https://myaccount.google.com/privacy.
>
> Google also offers a browser add-on that allows you to opt out of Google Analytics:
>
> https://tools.google.com/dlpage/gaoptout.[31]

The University of Michigan Library's policy provides three alternatives on how one can opt out of Google tracking.[32]

Notes

1. American Library Association, *Resolution on the Retention of Library Usage Records* (Chicago: American Library Association, 2006), 1, https://alair.ala.org/bitstream/handle/11213/1594/52.4.4%20Retention%20of%20Library%20Records.pdf.
2. American Library Association, "Developing or Revising a Library Privacy Policy," Privacy Tool Kit, last updated April 2017, www.ala.org/advocacy/privacy/toolkit/policy.
3. American Library Association, "Developing or Revising."
4. American Library Association, "Privacy and Confidentiality Q&A," last updated July 29, 2019, www.ala.org/advocacy/intfreedom/privacyconfidentialityqa.
5. American Library Association, *Privacy: An Interpretation of the Library Bill of Rights* (Chicago: American Library Association, 2002, amended 2014, 2019), www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy.
6. American Library Association, "Library Privacy Checklist for E-Book Lending and Digital Content Vendors," last updated January 26, 2020, www.ala.org/advocacy/privacy/checklists/ebook-digital-content.
7. American Library Association, "Library Privacy Guidelines for Vendors," last updated January 26, 2020, www.ala.org/advocacy/privacy/guidelines/vendors.
8. University of Miami Libraries, "Privacy Policy," https://www.library.miami.edu/about/privacy-policy.html.
9. University of California Los Angeles Library, "Privacy Policy," https://www.library.ucla.edu/use/access-privileges/privacy-policy.
10. Beaufort County Library, "Website User Agreement," 2009, https://2f26905f-7709-4fc5-8602-f82d730cafe1.filesusr.com/ugd/a57334_001fd0492b624dd386bc22e42903daf2.pdf.
11. East Greenbush Community Library, "Privacy Policy," https://eglibrary.org/about/policies/#privacy.
12. Musser Public Library, "Confidentiality Policy," August 19, 2015, https://musserpubliclibrary.org/wp-content/uploads/2018/08/Confidentiality-Policy.pdf.
13. Genesee District Library, "GDL Policy 5.5: Donations, Grants and Monetary Gifts," *Policy Manual* (Flint, MI: Genesee District Library, 2016), https://www.thegdl.org/wp-content/uploads/Policies/Policy-Manual-for-Website.pdf.
14. Phoenix Public Library, "E-Privacy," June 15, 2010, https://www.phoenixpubliclibrary.org/AboutUs/Documents/Policies/E-Privacy.pdf.
15. Cornell University Library, "Library Practices on the Collection, Use, Disclosure, Maintenance and Protection of Personally-Identifiable Information," https://www.library.cornell.edu/practices.
16. Montana State University Library, "Montana State University Privacy Policy," www.lib.montana.edu/privacy-policy/.
17. Cornell University Library, "Library Practices."
18. International Coalition of Library Consortia, *Privacy Guidelines for Electronic Resources Vendors* (International Coalition of Library Consortia, 2002), https://icolc.net/statement/privacy-guidelines-electronic-resources-vendors; American Library Association, *Code of Ethics of the American Library Association* (Chicago: American Library Association, 1939, amended 1981, 1995, 2008), www.ala.org/advocacy/sites/ala.org.advocacy/files/content/proethics/codeofethics/Code%20of%20Ethics%20of%20the%20American%20Library%20Association.pdf.
19. Harvard Library, "Harvard Library's Privacy Statement," Privacy, Terms of Use and Copyright Information, https://library.harvard.edu/privacy-terms-use-copyright-information#privacy.
20. Stanford Libraries, "Statement on Patron Privacy and Database Access," https://library.stanford.edu/using/special-policies/statement-patron-privacy-and-database-access.
21. Duke University Libraries, "Duke University Libraries Privacy Statement," https://library.duke.edu/about/privacy.
22. Brown County Library, "Privacy and Confidentiality," May 15, 2014, https://www.browncountylibrary.org/wp-content/uploads/2012/09/H_1-Privacy-and-Confidentiality.pdf.
23. Nashville Public Library, "Social Media and Blog Guidelines for Using, Commenting, and More," https://library.nashville.org/about/policies/social-media-and-blog-guidelines.
24. Nashville Public Library, "Privacy Notice," last updated May 2, 2016, https://library.nashville.org/privacy-notice.
25. Los Angeles Public Library, "Online Privacy Policy," last updated March 2018, https://www.lapl.org/online-privacy-policy.
26. Rutgers University Libraries, "Privacy Policy," October 19, 2010, https://www.libraries.rutgers.edu/privacy_policy.
27. University of North Carolina at Chapel Hill Libraries, "Privacy Policy," last updated March 19, 2018, https://library.unc.edu/about/policies/privacy-policy/.
28. Utah State University Libraries, "Utah State University Libraries Privacy Statement," https://arwen.lib.usu.edu/privacy_policy/.

29. Cornell University Library, "Library Practices."
30. University of California Berkeley Library, "Collection, Use, and Disclosure of Electronic Information," last updated September 22, 2008, https://www.lib.berkeley.edu/about/privacy-electronic-information.
31. University of Denver Libraries, "Your Privacy and University Libraries," https://library.du.edu/policies/records-privacy.html.
32. University of Michigan Library, "Library Privacy Statement," last updated March 2016, https://www.lib.umich.edu/library-administration/library-privacy-statement.