Collaborative Librarianship

Volume 9 | Issue 1 Article 2

March 2017

Protecting Patron Privacy: Vendors, Libraries, and Patrons Each Have a Role to Play

Lori Bowen Ayre
Galecia Group, lori.ayre@galecia.com

Column Name: Technology Matters

Protecting Patron Privacy: Vendors, Libraries, and Patrons Each Have a Role to Play

Abstract: Protecting patron privacy involves several activities including responsibly managing the data we store about patrons and their use of the library as well as working with our vendors which also access and make use of that data. It also involves educating our patrons so they can better control what happens with their personal information.

Our commitment to protecting our patron's intellectual property is a guiding principle in the ALA Code of Ethics stating that librarians "protect each library user's right to privacy and confidentiality with respect to information sought or received, and resources consulted, borrowed, acquired, or transmitted." The ALA Code of Ethics was originally adopted in 1939 before MARC records, the integrated library system, and definitely before the Internet. It is much more complicated to protect our patron's privacy today than it was in 1939. However, it is timely to revisit the issues around patron privacy as we embark on our journey with the new administration.

According to the ACLU Trump Memos (http://bit.ly/2gJvdok), and now confirmed by Executive Orders, we are dealing with an Administration that uses religion to justify surveillance, is threatening to deport large numbers of members of our communities, and has redefined accepted definitions of freedom of expression and libel. It is more important than ever to know how to protect our patron's privacy.

The Library Side

On December 5, 2016, the Electronic Frontier Foundation posted an article entitled "Librarians, Act Now to Protect Your Users (Before It's Too Late)" (http://bit.ly/2gJtmA5). The article is instructive and provides some specific steps that libraries should take to protect their users' intellectual privacy including:

- Limit collection and retention of user information. Only collect the minimum amount of information necessary to provide a service and don't keep that information any longer than necessary.
- Follow best practices for anonymizing any information that is retained
- Allow anonymous use of library services whenever possible
- Make sure staff know how to deal with governmental requests (Note: ALA has a good site with more detail on this issue. See http://bit.ly/2gDYy3u).
- Use HTTPS (provides for encrypted communications over the Internet) for the library website at all times, and push vendors to do the same
- Limit the use of cookies (used to track users' preferences and activities) and make cookies "opt in". The library website should also be able to be used without cookies.
- Secure library computer browsers with built-in privacy protections and enable extensions like EFF's Privacy Badger and HTTPS Everywhere. Keep both the browsers and extensions up-to-date.

- Require third-party vendors to match library privacy practices for patron data

The Vendor Side

Many of the services libraries use to deliver content to patrons (e.g. aggregated databases, ebooks, and other digital content) and the integrated library system (ILS) itself relies on user data to improve its service offerings. Like so many services online, these services track and collect information about users, and analyze user behavior. This information isn't under the control of the library but it might be information that could be demanded by law enforcement.

In 2015, NISO (National Information Standards Organization) hosted a series of discussions to address the complex relationship between library service providers and librarians for the purpose of formulating a framework that would strike the right balance between privacy protection and using patron usage data to improve library services. NISO received a grant from the Andrew W. Mellon Foundation to pursue this work and to develop what they called a "Consensus Framework to Support Patron Privacy in Digital Library and Information Systems."

After many passionate discussions and conference calls and all day meetings, the group (this author was a core member) was able to find their way through the digital ecosystem in which libraries currently operate to develop 12 principles that form the foundation for developing practices and procedures that protect the digital privacy of library users. The resulting document, *NISO Consensus Principles on User's Digital Privacy in Library, Publisher, and Software-Provider Systems (NISO Privacy Principles)* is available at the following (ironically un-encrypted) URL: http://bit.ly/2gGHcD6 and is summarized below:

1. Shared Privacy Responsibilities

Publishers and software-providers, which operate through and for the library and its users, share in the ongoing ethical responsibility of protecting patron privacy. Anyone with access to library data and activity should accept responsibility for safeguarding user privacy and data security and should have training in related standards and best practices.

2. Transparency and Facilitating Privacy Awareness

Library users need to be able to determine the extent of privacy protections provided and the boundaries of those protections as they use library resources. This means providing information about how and what information is used in a way that they can understand it, and informing library users what they can do for themselves to protect their privacy.

3. Security

The baseline to protect data should be based on the most current security best practices including encryption of personal data; prompt updates of systems and software to address vulnerabilities; systems, procedures, and policies for access control of sensitive data; security training; and documented procedures for breach reporting, incident response, and system, software, and network security configuration and auditing.

4. Data Collection and Use

The potential benefit derived from the collection and use of users' personal data must be balanced against the impact of that collection and use on users and their right to privacy. Users' personal data should only be used for purposes disclosed to them and to which they consent.

5. Anonymization

Personally identifiable information should be retained in that form only as long as absolutely necessary for operational purposes. Anonymization should be used as part of a broad set of information privacy controls that include: data minimization; statistical disclosure limitation methods, such as controlled aggregation; data-use agreements; and auditing. Anonymization may not completely eliminate the risk of re-identification; therefore, even anonymized raw data should be treated with precautions in proportion to the potential risk of re-identification.

6. Options and Informed Consent

Each library user's needs and expectations of privacy are different and may be contingent on circumstances. When personal data are not required to provide services, library users should have options as to how much personal information is collected and how it may be used. The default approach/setting should be that users are opted out until they explicitly choose to opt in but they should have the option to opt-in later.

7. Sharing Data with Others

Parties must carefully consider the impact on the user's privacy before sharing data or information with third parties. Considerations should include: the library user's consent; the user's privacy interests; any legal prohibitions or requirements; the policies of that third party and their adherence to these principles; and the risks and benefits to the user and institution.

Shared user activity data should be anonymized and aggregated to a level that minimizes privacy risks to individual users, unless the user has opted-in to a service.

8. Notification of Privacy Policies and Practices

Privacy policies should be made easily available and understandable to users and when the policies change, users should be notified.

9. Supporting Anonymous Use

Reasonable accommodations to provide basic services should be made for users that choose to remain anonymous. When the collection and retention of a user's personal data are required in order to access library resources or deliver library services, the library user should be informed that anonymous service is not possible.

10. Access to One's Own User Data

Users should have the right to access their own personal information or activity data. Users should be provided, in so far as is feasible, access to these data for review, so that users may request correction or deletion.

11. Continuous Improvement

Libraries, content-, and software-providers should continuously assess and strive to improve user privacy as threats, technology, legal frameworks, business practices and user expectations of privacy evolve.

12. Accountability

Libraries, content-, and software-providers should establish a culture of accountability in which data collection, security, use, sharing, and disposal practices and policies are reviewed and reported on a periodic basis.

Data privacy in the digital age is a complicated business. It goes way beyond making sure your library doesn't keep a record of what your patrons have checked out. Luckily, the ALA's Intellectual Freedom Committee updated many of the resources available on the ALA website (http://www.ala.org/advocacy/privacyconfidentiality). The updated information includes library privacy guidelines for E-book lending and digital content vendors; data exchange between networked devices and services (e.g. APIs, SIP2, Z39.50); public computers and networks; websites, OPACs and discovery services; integrated library systems; and students in K-12 schools.

Each guideline also includes a link to detailed checklists (just updated in 2017) that "take the theoretical principles around privacy and organize them as practical actions that libraries of any capacity can take to protect their patrons." These checklists are organized into three "Priority Action" categories. Priority 1 Actions are steps that most libraries can implement while Priority 2 and 3 may require more technical expertise on staff. Examples of Priority 1 Actions include:

- Limit the amount of personal information collected about users
- Provide links to vendor privacy policies
- Work with vendors to configure services to use opt-in methods whenever possible
- Develop a strategy to assist patrons in managing their privacy when using vendor products and services.
- Provide users with options as to how much information is collected from them and how it is used

The checklist pages also include useful resources and additional questions library staff should consider in implementing the guidelines.

Another excellent resource for current privacy information is the blog from the Choose Privacy Week initiative (https://chooseprivacyweek.org/blog/). This initiative has been around since at least 2010 and was launched for the purpose of "engaging people in a national conversation about privacy rights in a digital age." The resources there are targeted educating patrons about privacy issues so they can make more informed choices about their own privacy.

Privacy matters continue to get more complicated as more and more of our information moves online, as we share information with service providers and as the demands for customized services that rely on personal information grow. It is important the librarians continue to educate themselves and ensure their institutions are doing what needs to be done to protect our patrons from surveillance or any kind of unwanted attention from the powers that be. This is no small task, and it requires cooperative efforts at every level of the organization but it is a fundamental principle of our profession so it is important to do the work necessary. Especially now.