Privacy in Public Libraries

Bill Marden, Director of Privacy and Compliance, The New York Public Library

Greg Cram, Associate Director of Copyright and Information Policy, The New York Public Library

Privacy. The subject of how our personal information—including some of the most intimate details of our daily lives—gets used and sometimes abused has become a common topic in the media and in daily conversations. Americans and the world at large are trying to come to grips with a new paradigm that determines what is and what can be known about all of us through the collection of data in all its forms. Congress has made this topic a key area of focus in its current session. Senator John Thune (R-SD), Majority Whip, opened a pair of hearings last fall by stating that developing a privacy law for the United States enjoys bipartisan support. All signs point to Congress taking on the issue of privacy over the next two years, but it is not clear yet what shape the privacy law will take. As Congress develops a comprehensive privacy proposal, libraries will play a critical role in shaping that law. This article illuminates the challenges faced by public libraries, elucidates the role of libraries in the privacy landscape, and identifies new projects designed to help libraries respond to the privacy challenges presented by new technology.

> “Public libraries face myriad privacy challenges, both external and internal.”

Today, public libraries face myriad privacy challenges, both external and internal. There is a constant need to assess and use the data that libraries routinely collect and store. Data, whether in its old-fashioned analog form (think paper call slips) or digital, is a desirable and highly sought-after commodity in our current world. On the more benevolent side of this usage is data analytics used by libraries to determine the effectiveness of their programs and resources. On the less benevolent side is the use of such data for surveillance or crime solving by law enforcement, or the possible unauthorized use by third-party vendors. For example, law enforcement may seek video recordings from security cameras to collect information about an alleged crime. A database vendor might resell data about a patron or might market to a patron without the library's permission. On the truly darker side is the ever-present danger that library data could be stolen (and occasionally held ransom) by hackers or unwittingly left out in the open, available for anyone to discover it. Finally, when libraries strive to provide improved, more-personalized services tailored to their patrons, they often find themselves forced into making difficult, ethical choices about the use of cutting-edge technology that easily allows them to track and analyze how, where, and when patrons are using library materials. If a library is offering a program on a topic that is likely to be of interest to a particular patron, how might the library target an email to that patron (aside from the patron proactively signing up to receive such notices)?

These scenarios raise important privacy and confidentiality challenges, including a patron's right to opt in and opt out of how and when the library collects her personal information. Although we often use the words privacy and confidentiality interchangeably, there is a distinct difference between the two concepts. Privacy, by definition, is an individual's right to control the collection, use, and disclosure of personal information. For example, an individual makes certain decisions about her privacy when seeing a doctor for an exam. The individual grants permission to the doctor to conduct an examination that will reveal personal information to the doctor about the individual's health. Confidentiality, on the other hand, is the obligation of an individual, organization, or business to protect personal information and not misuse or wrongfully disclose that information. In the example of the doctor visit, the doctor has a duty of confidentiality to protect the information learned during the individual's exam and must abide by the patient's decisions about what information, to whom, and when it can be shared.

Foundations of Privacy in Libraries

Libraries facing these challenges can look to the principles of the profession to understand how to collect and disseminate information about their patrons. Since 1939, the American Library Association (ALA) has affirmed the right of privacy for library patrons. Article 11 of the original Code of Ethics for Librarians states, "It is the librarian's obligation to treat as confidential any private information obtained through contact with library patrons."[1] The current Code of Ethics states, "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."[2] Patron privacy is crucial to freedom of inquiry and access to library resources for all users. ALA's Intellectual Freedom Committee and its Privacy Subcommittee have worked to provide forums and guidelines, and act as a clearinghouse for library privacy issues and ideas, including the annual Choose Privacy Week, a privacy section in the weekly *Intellectual Freedom News*,[3] and a website: chooseprivacyeveryday.org.

> "Since 1939, the American Library Association (ALA) has affirmed the right of privacy for library patrons."

Beyond the principles of the profession, all libraries are subject to state laws that dictate how personal data can be collected and used within libraries specifically. In the 1980s, states began passing statutes protecting the confidentiality of library records. New York State passed such a statute in 1981 that prohibits the disclosure of library records and prohibits their use "except when necessary for the proper operation of the library" and in response to subpoenas, warrants, and law enforcement requests. The legislators who wrote the bill noted in their supporting documentation:

> The library, as the unique sanctuary of the widest possible spectrum of ideas, must protect the confidentiality of its records in order to insure its readers' right to read anything they wish, free from the

> fear that someone might see what they read and use this as a way to intimidate them....Without such protection there would be a chilling effect on our library users as inquiring minds turn away from exploring varied avenues of thought because they fear the potentiality of others knowing their reading history.[4]

By affirming that privacy is an essential value of American libraries, the New York State legislature provided the means and authority for libraries to truly protect the personal information of their patrons.

New Technology and Privacy

Innovations in technology have created—and continue to create—new privacy challenges for public libraries. The amount of personal data that can conceivably be collected today, compared to even a decade ago, is monumental. For example, by employing commercially available marketing tools, libraries can now track how patrons are engaging with a library's website and the websites of others. This information could potentially be used to target ads and announcements toward specific users to inform them of programs or events that are likely to be of interest. The question is whether libraries **should** make use of such technologies simply because they are legally available and because they are used in the larger world of marketing and commerce.

> "Innovations in technology have created—and continue to create—new privacy challenges for public libraries."

Current Projects

Given the ease with which such information can be collected, libraries are on the forefront of creating privacy-related training and procedures to help safeguard personal information. ALA's Privacy Subcommittee and ALA's Library Information Technology Association (LITA) both hold regular forums and presentations on privacy at ALA's Annual Conference and through webinars and other programs throughout the year. State and regional library associations, graduate school library science programs, and the academic community (including academic journals, such as *RLI*) are also increasingly engaged in this topic. In addition, various external grant-making organizations are funding privacy projects. In 2017, the Institute of Museum and Library Services (IMLS) awarded a grant to the Center for Information Policy Research at the University of Wisconsin–Milwaukee in partnership with Data & Society, ALA's Office of Intellectual Freedom, and The New York Public Library. The grant made it possible to host a series of meetings, including a national forum in May 2018 to explore what privacy means in the digital world. The grant investigators identified a set of common themes that summarized the growing need and challenges to maintain libraries' commitments to patron privacy.[5]

> "Libraries are on the forefront of creating privacy-related training and procedures to help safeguard personal information."

Other recent grant awards have focused on training public librarians to become privacy leaders at their institutions. Funded by IMLS, New York University and Library Freedom Project have launched the Library Freedom Institute, a six-month train-the-trainers course for librarians.[6] The participants spend time each week learning how to install and use privacy software, educate communities on privacy practices, promote privacy as a design principle within their libraries, and advocate for privacy-first policies and legislation. In what is perhaps the largest, most-encompassing library-privacy initiative in the country, the three major New York City library systems—New York Public Library, Brooklyn Public Library, and Queens Library—joined together to create the NYC Digital Safety: Privacy & Security training program in 2018.[7] The ongoing program trains New York City's front-line librarians in preparing them to answer questions from New Yorkers about how to safely navigate the world of digital information. As the project's manager, Davis Erin Anderson, noted during the program's launch:

> Many New York City residents use digital technology nearly every waking hour of their day. From using email at work to browsing social media on the subway to streaming television shows at home, we are consistently delivering a wealth of data about who we are and what we do online to Internet Service providers and myriad online entities. This information can be utilized to influence our behavior, and, more pressingly, can be used against us in the event of, for example, a successful phishing attempt or a data breach.[8]

The NYC Digital Safety project received financial support from the City of New York and was overseen by the Metropolitan New York Library Council (METRO). It resulted in a set of online modules that are now freely available, not just for librarians, but for anyone to use. The topics cover a wide range of basic information, including:

1. Introduction to Digital Safety
2. Internet Technologies and the Information Flow
3. Who Collects Data; Connecting Securely
4. Securing Accounts and Devices
5. Preventing Tracking
6. Avoiding Scams and Malware; Minimizing Your Digital Footprint
7. Privacy and Security in the Library

For more information see nycdigitalsafety.org.

In late April 2019, METRO announced that it would be launching a second phase of this project, which will include updates to the existing online modules, a program to bring library staff together to implement a public-facing approach to online privacy, an NYC Library Privacy Week planned for the fall of 2019 and 2020, and a one-day Privacy Summit for New York City's public library staff.

NYPL Initiatives

The New York Public Library is also paving the way in creating other privacy standards and controls that meet the demands of the 21st-century library. The data that flows through most modern libraries, one could argue, is actually in the hands of third-party vendors. Many products and services the library depends on, such as integrated library systems (ILS), customer relationship management (CRM) databases, software programs for educational use, analytics software, cloud storage, and website hosting, are outside the library's direct and complete control and rely on contractual agreements. The question for libraries is how to best control these agreements and outside relationships. NYPL has a workflow that involves the director of privacy, the legal department, IT, and a risk manager from purchasing in reviewing any vendor contracts that involve the collection and use of personally identifiable information (PII) about patrons, making certain that that PII is safeguarded and properly controlled by the vendor throughout the data life cycle (starting from the point of collection, to its storage, its access, and ending with its proper retention and disposal).

> The New York Public Library is also paving the way in creating other privacy standards and controls that meet the demands of the 21st-century library.

NYPL also proudly boasts that it is the first and (still) only library in the country to have a full-time privacy officer, a position which has existed here since 2015. In his role as NYPL director of privacy and compliance, Bill Marden has formed a Privacy Advisory Committee comprised of representatives from every division of the library, who meet monthly to discuss and help decide various initiatives and issues related to privacy at NYPL. With the help of the members of this committee, NYPL is embarking on a complete inventory of its data-collection practices, including a risk assessment of how well the library safeguards data containing PII.

Conclusion

Protecting the privacy of patrons remains an essential principle for public libraries. The commitment to this principle is regularly challenged by a variety of pressures, including the ease of data collection and dissemination created by technological advances. Although these challenges are sharpened by technology, libraries can draw on their history of offering a sanctuary for intellectual freedom. New projects focusing on understanding these pressures and training librarians will help guide public libraries through these challenges.

Endnotes

1. 1939 Code of Ethics for Librarians, American Library Association, accessed April 30, 2019, http://www.ala.org/Template.cfm?Section=coehistory&Template=/ContentManagement/ContentDisplay.cfm&ContentID=8875.

2. Code of Ethics of the American Library Association, ALA, last amended January 22, 2008, http://www.ala.org/advocacy/sites/ala.org.advocacy/files/content/proethics/codeofethics/Code of Ethics of the American Library Association.pdf.

3. *Intellectual Freedom News*, Office for Intellectual Freedom, American Library Association, accessed April 30, 2019, https://www.oif.ala.org/oif/?cat=393.

4. Memorandum of Assemblyman Sanders, *New York State Legislative Annual 1982* (New York: New York Legislative Service, 1982), 25, cited in Quad/Graphics, Inc. v. Southern Adirondack Library System, 174 Misc. 2d 291, 294 [Sup. Ct. 1997], https://caselaw.findlaw.com/ny-supreme-court/1481617.html.

5. "Project Report: 'Library Values & Privacy in Our National Digital Strategies: Field Guides, Convenings, and Conversations,' " Center for Information Policy Research, University of Wisconsin–Milwaukee, August 2, 2018, https://cipr.uwm.edu/2018/08/02/project-report-library-values-privacy/.

6. Library Freedom Institute website, accessed April 30, 2019, https://libraryfreedomproject.org/lfi/.

7. NYC Digital Safety: Privacy & Security website, accessed April 30, 2019, https://nycdigitalsafety.org/.

8. Davis Erin Anderson, "New Privacy Resources Available from NYC Digital Safety," *Voices for Privacy Blog*, December 5, 2018, https://chooseprivacyeveryday.org/new-privacy-resources-available-from-nyc-digital-safety/.

To cite this article: Bill Marden and Greg Cram. "Privacy in Public Libraries." *Research Library Issues*, no. 297 (2019): 38–46. https://doi.org/10.29242/rli.297.4.