**Online Privacy Protection and Public Libraries: A Review of Contemporary Research**

Shelby Thomas
School of Library and Information Management, Emporia State University
LI810XM: Research
Dr. Jinxuan Ma
May 7th, 2022

**Introduction**

Over the last three decades, public libraries have been challenged with staying relevant amidst a rapidly evolving technological landscape. As the world has become increasingly connected and online technologies have improved, the public library has had to adapt apace with librarians and information professionals needing to be educated in new methodologies and changing technology standards along the way. The library is there to serve the public, and as technology evolves, the public's expectations of their community library grow. The modern public library is thus expected to maintain a thoroughly capable information and communications hub for their community.

With the advent of social media in the last decade and because online activity now affects virtually every part of our lives, the susceptibility of internet users to the unauthorized collection of their private information has never been more pronounced. Speaking at the Lake Superior Libraries Symposium in 2016, Jason Griffey proclaimed that there might not be a public library service more important than privacy in the future (Gardner, 2021). The International Federation of Library Associations and Institutions (IFLA) has deemed privacy and technology the primary trends in the information science landscape (IFLA, 2016 as cited in Kritikos & Zimmer, 2017). Researcher and legal librarian Sarah Shik Lamdan (2015) believes that librarians and the ALA are "the best potential sources of intellectual freedom advocacy in the Internet age," (p. 262). Public libraries have always been fierce protectors of the private information of their patrons—as outlined in the American Library Association's *Code of Ethics* (American Library Association [ALA], 2021)—so their mission to provide robust information services to the community requires that public libraries also devote significant time, resources, and personnel to the problem of online privacy protection. The kind of access patrons want tends to require that they share their private information with third parties (Litwin, 2014).

The degree to which public libraries have been successful in defending the online privacy of their patrons is difficult to ascertain from an historical perspective—apart from a handful of small-scale data breaches, there is simply little known about how much data has been collected from online users of public libraries. There is also a dearth of information and research regarding how best to calculate and evaluate trade-offs between providing electronic resource access and allowing certain compromizations of patron privacy (Litwin, 2006, as cited in Rubel, 2014). There has, however, been research into how well-prepared public libraries are to meet known threats to user privacy. This paper presents the findings of several such studies in an effort to elucidate the current preparedness level of public libraries in terms of meeting online privacy protection standards. More broadly, it is a qualitative review of contemporary literature examining the various ways public libraries are handling patron privacy issues. It is believed that this may be of particular use to public librarians inclined to examine their own institutions' privacy policies and practices.

## Literature Review

### Identifying the Problem(s)

One of the reasons protecting the privacy of patrons is a difficult issue is that it cannot be adequately described as simply one problem. It is rather a collection of problems, each of which represents but one facet of a complex system of variables and vulnerabilities. To deal with privacy protection effectively, a library must confront several individual problems. This part of Section I is a review of the most salient and pressing of these problems and complicated realities.

The first of these is the reality that the public library is bound by their principles to protect and defend the privacy and private information of their patrons. As mentioned, the ALA's *Code of Ethics* explicitly 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," (ALA, 2021). In an interpretation of Article VII of the *Library Bill of Rights*, the ALA further states "All people...possess a right to privacy and confidentiality in their library use," and reveals the stakes involved by explaining that "When users recognize or fear that their privacy or confidentiality is compromised, true freedom of inquiry no longer exists," (ALA, 2020). As Lambert et al. note (2015), access to information is effectively restricted and compromised when the knowledge of potential surveillance hangs over the information seeking process. Also noteworthy in this regard is that some research indicates the average internet user is very much interested in protecting their privacy and wresting control over their personal information (Madden and Rainie, 2015, as cited in Maceli, 2019). And according to a Pew Internet Center poll, 86% of US citizens make an effort to conceal their identities when using the internet (Pew Research Center, 2013, as cited in Lamdan, 2015).

This presents a problem for libraries because to offer modern information platforms and online technology services is to expose patrons to the potential collection of their personal information and private data against their will. Libraries must therefore offer their communities substantial protection and a capable defense against violations of patron privacy along with these online services.

One avenue for the potential collection of patron data involves e-services. The introduction of digital lending services to public libraries has also introduced other service providers into the process which very often do not have comparable concerns for privacy and indeed fail to meet the privacy standards of libraries. When an e-book is accessed, for instance, there are two parties in addition to the library who can collect patron data: the e-reader company and the service vendor. Research by Lambert et al. (2015) suggests that librarians involved in contract negotiations should ensure that vendors are

aware of the privacy expectations in the library profession and their differences with the privacy standards of the broader information technology industry. Amazon's Kindle e-book lending service requires that users create and log in to a Kindle account, which allows Amazon to track the user's borrowing practices. Alan Rubel points out (2014) that libraries who choose to lend books via the Kindle service effectively put themselves in the awkward position of admitting to users that the library's privacy policy can't protect them here.

From a general standpoint, usage of internet services through the public library represents a huge liability to patron privacy. Social media is particularly troublesome because it has become the public's primary source for news and online communication and it collects a great deal of metadata from users. Sarah Shik Lamdan explains (2015) that social media user data can consist of biographical information, personal affiliations, private messages, individual clicks, “likes,” videos, photos, GPS location data, access logs, and more. She also states that the onus is rather squarely on librarians to champion the cause of user privacy due to the federal government failing to adequately address privacy issues that have come about in the age of social media—there is currently no federal response in the national legal framework to the privacy compromizations that occur due to social media use. Furthermore, this lack of federal statutes regarding internet privacy has allowed social media providers free reign when it comes to collecting their users' private data (Lamdan, 2015).

Many libraries have implemented or are implementing third-party cloud computing platforms and tools into their services. Examples of these include OCLC WorldShare, Ex Libris Alma, and BiblioCommons. These platforms provide a more user-focused experience for exploring library materials, incorporating social media-style interactions and data-driven tools. They are largely based on the aggregation and tracking of usage and activity data, which represents another way patron privacy is compromised for the sake of providing enhanced library services (Kritikos & Zimmer, 2017). Third-party tracking, however, is often invisible to libraries, occurring on websites external to the institution's user

service platforms. CSU Longbeach librarian and researcher Gabriel J. Gardner (2021) explains that third-party tracking has been a common and ubiquitous trait of the modern internet since first appearing in 1996. It is almost exclusively used for commercial purposes, especially targeted advertising. Preventing this kind of data collection can at times be next to impossible, so libraries need to be up front about this reality with users by virtue of online messaging and they must make effective use of privacy-protection technologies that can prevent third-party tracking. Gardner's research revealed that, out of the 178 North American (133 from the US, 45 from Canada) public libraries sampled, 154 were found to have third-party tracking present in their online catalogs.

A major hurdle for protecting patron privacy has been that many libraries and librarians have struggled to remain current on the latest trends and developments on privacy-protection measures and technologies in the information landscape. A 2015 study suggests that the knowledge and education level of librarians is full of noteworthy gaps when it comes to the internet, cloud computing, the reselling of users' private data by corporations, and privacy-protection technologies (Bashir, as cited in Maceli, 2019). Research conducted by Monica Maceli (2019) even indicates that traditional training and education methods on privacy aren't producing results. She states that the information science field needs teaching technologies and education methods that have a greater impact on one's online privacy behaviors and decision making.

The final problem identified by this research is that public libraries tend to have insufficient, out-of-date, or ineffective privacy policies. Emporia State researcher Brady D. Lund (2021) studied a random sample of 1000 public libraries and analyzed their approaches to data privacy. He found that, out of the 1000 sampled, 554 of the public libraries studied had no data privacy statement on their website. He further notes that although the ALA's Library Bill of Rights is the main and most prominent source from which intellectual freedom ideas and values are derived, relatively few (28%) of those libraries with online privacy policies mention it. Adult Services Librarian T.J. Lamanna (2019) contends that even while

a given public library may have a privacy policy, many policies are weak, and staff are often not sufficiently trained in the policy details.

**Current Approaches**

A study by Kritikos and Zimmer (2017) showed that, while most of the thirty-four libraries participating in BiblioCommons third-party cloud computing services did not update their privacy policies after adopting BiblioCommons, a handful (8) did. This can be identified as a best practice—whenever any changes to a library's services happen, a revisitation of the privacy policy (and all posted versions of it) should always occur. Their study reveals what they consider an uneven approach to ensuring there is agreement between internal policy and technological changes to library services. Indeed, the ALA (2020) recommends that public libraries routinely conduct privacy audits to address potential privacy gaps with regard to patron services.

One way the library profession is addressing patron privacy concerns is through grant-funded projects focusing on training public librarians to become champions of privacy protection. The Institute of Museum and Library Services (IMLS) funded such a project that was spearheaded by New York University and the Library Freedom Project in 2018 called NYC Digital Safety: Privacy & Security. It is a six-month course which trains front-line librarians to answer patron questions about privacy protection and safe internet practices. Participants learn how to use privacy protection tools, how to promote privacy as a design principle, and how to advocate effectively for legislation that protects the privacy of citizens (Marden & Cram, 2019). Continuing education is becoming increasingly important when it comes to the issue of privacy in public libraries—the tech landscape changes frequently, so routinely updating the knowledge levels of public-facing librarians is necessary to maintain a high level of

helpfulness to the public. Joshua Becker of Southern New Hampshire University sees privacy training as an all-staff endeavor, suggesting that teaching privacy should not be a focus of only reference and liason librarians, but rather of all library employees (2021). Megan Maceli notes (2019) that many of the technological standards and privacy recommendations may have changed dramatically since many librarians received their degrees, so periodic privacy training is crucial.

A very simple, effective, and free measure public libraries can take for safeguarding the private information of their users is to use HTTPS for their library websites. It is called Transport Layer Security, and it authenticates websites and keeps them free of types of tracking like packet-sniffing and packet-injection. Using the outdated, unsecured HTTP allows for digital snooping that HTTPS takes care of, yet many libraries still serve their websites in it. Another free and easy change libraries can make is to have their browsers' search engines default to a privacy-friendly search engine like DuckDuckGo (Gardner, 2021).

Some of the findings of Brady Lund's research (2021) indicate that public libraries serving larger populations are more likely to reference pre-existing privacy guidelines (such as the Library Bill of Rights) in their privacy policy than those serving smaller communities. It furthermore showed that those policies which build from existing frameworks like the LBOR were generally the most detailed and effective policies. It can be reasonably presumed, then, that basing a privacy policy on an existing framework or set of guidelines will generally lead to more successful outcomes than would starting a privacy policy from scratch. So much of public library management is made simpler through relying on best practices, and maintaining an effective privacy policy seems to be no exception.

Libraries dealing with vendors and software companies in contract negotiations can ensure that companies with whom they enter into contracts abide by the privacy protection standards maintained by the library and outlined by the ALA. Librarians could influence social media platforms and tech companies to adopt privacy measures and apply them to their terms-of-service contracts. UK researcher

Paul Pedley (2017) suggests that contracts should require that libraries retain ownership of all data and that any third-parties used by the vender should be bound by the same requirements. Libraries can furthermore become involved in and supportive of legislation that deals specifically with the privacy issues affecting libraries. One such state law, enacted by California, requires social media providers to inform consumers as to whether or not they acknowledge “do not track” settings in web browser software (Lamdan, 2017). Libraries and librarians can use their public-facing platform to engender support among their patrons and community for such legislative proposals.

A theoretical method of protecting user privacy examined by Wu, et al. (2019) shows that privacy can be quite effectively protected in digital library services via a novel approach to encrypting user data. In their system, private data is first encrypted before submission to the library server. Query processing is then done at the server side without decryption, preserving user anonymity and privacy without compromising availability of service. Such technical approaches to protecting patron privacy can be transposed into effective privacy-protection tools, apps, extensions, or even platforms.

Another way libraries have been dealing with the problem of patron privacy protection is by providing the secure distributed network Tor as an alternative to traditional web browsers (like Chrome and Firefox). Tor and other web networks like it give users additional layers of anonymity and encryption, the effectiveness of which is impossible to achieve with web browsers. The Library Freedom Project provides information for libraries interested in utilizing Tor. Kilton Library in New Hampshire was the first library to host a Tor server, while the Lewis & Clark Library in Helena, Montana has offered Tor on its public computers for years. Tor's values seem to align quite strongly with those of public libraries (Lund & Beckstrom, 2021).

**Conclusion**

Protecting the privacy of public library users is at once a matter of ethics, one of founding principles (in terms of the ALA, specifically), and one of necessity—as risks to patron privacy inevitably grow, so must the capability and capacity of public libraries to protect that privacy. And there are obstacles in the way which may further complicate matters. One of these obstacles is that two generations of users—Generation Z and Millenials—potentially harbor defeatist, cynical attitudes toward privacy protection. Recent studies have indicated that less than one third of both groups considered themselves very concerned about data privacy. This represents quite a departure from the Generation X demographic, two thirds of whom think secure internet communication is important (Becker, 2021). Informing and educating these patrons on privacy matters and developing a sense of urgency in them may be an uphill battle.

Another of these obstacles is political. Regardless of how effective at protecting patron privacy a library is in the present, Stavroula Harissis (2017) warns that merely demonstrating the value of libraries may not be enough to secure public funding in the future, thereby making it harder for libraries to fulfill their mission of protecting patron privacy. Written during the Trump administration, her piece describes an economic and political climate marked by neoliberalism, in which a government's actions are dictated and decided by what is found to be most beneficial to markets. Government policies are strengthening the private sector (via corporate tax breaks and deregulation) while effectively weakening the public sector. As she titles one section, “Neoliberalism Wants Libraries to Fail,” (p. 6). We can currently see the upcoming elections on the horizon, and it doesn’t look promising for those in favor of a healthy, well-funded public sector in which public libraries can efficiently manage the problem of patron privacy.

The years ahead may test the mettle of librarians with a financial climate in which “doing more with less” might be a particularly practical idiom. Novel, cost-saving approaches can materialize in such

climates; practices like implementing the free and opensource Tor over traditional web browsers, defaulting to privacy-friendly search engines, and doing routine privacy protection audits are potentially more viable ways forward than those which might require additional funding. Public libraries may find themselves negotiating vendor contracts from weaker positions than they have in the past due to corporate-friendly political machinations in play, so staying active and abreast of privacy-related legal and legislative issues will be imperative for librarians.

**References**


American Library Association. (2021, July 21). *Professional ethics.* Retrieved April 26, 2022, from https://www.ala.org/tools/ethics

American Library Association. (2020, February 5). *Privacy: An interpretation of the library bill of rights*. Advocacy, Legislation & Issues. Retrieved April 28, 2022, from https://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy

Becker, J. (2022). Promoting library services in an age of data insecurity. *Serials Librarian*, *81*(1), 8–10. https://doi-org.proxy.library.umkc.edu/10.1080/0361526X.2021.1875963

Cooke, L. (2015). Importance of users' privacy in library public internet access. *Multimedia Information & Technology*, *41*(4), 19–22.

Gardner, G. J. (2022). Aiding and abetting: Third-party tracking and (in)secure connections in public libraries. *Serials Librarian*, *81*(1), 69–87. https://doi-org.proxy.library.umkc.edu/10.1080/0361526X.2021.1943105

Harissis, S. (2017). The fight for public library funding: Demonstrate value or demonstrate in the streets? *Progressive Librarian*, *46*, 5–11.

Kritikos, K. C., & Zimmer, M. (2017). Privacy policies and practices with cloud-based services in public libraries: An exploratory case of BiblioCommons. *Journal of Intellectual Freedom & Privacy*, *2*(1), 23–37. https://doi-org.emporiastate.idm.oclc.org/10.5860/jifp.v2i1.6252

Lamanna, T. J. (2019). On educating patrons on privacy and maximizing library resources. *Information Technology & Libraries*, *38*(3), 4–7. https://doi-org.proxy.library.umkc.edu/10.6017/ital.v38i3.11571

Lambert, A. D., Parker, M., & Bashir, M. (2015). Library patron privacy in jeopardy. *Proceedings of the Association for Information Science & Technology*, *52*(1), 1–9. https://doi-org.emporiastate.idm.oclc.org/10.1002/pra2.2015.145052010044

Lamdan, S. S. (2015). Social media privacy: A rallying cry to librarians. *Library Quarterly*, *85*(3), 261–277. https://doi-org.proxy.library.umkc.edu/10.1086/681610

Lund, B., & Beckstrom, M. (2021). The integration of Tor into library services: An appeal to the core mission and values of libraries. *Public Library Quarterly*, *40*(1), 60–76. https://doi-org.proxy.library.umkc.edu/10.1080/01616846.2019.1696078

Lund, B. D. (2022). Public libraries' data privacy policies: A content and cluster analysis. *Serials Librarian*, *81*(1), 99–107. https://doi-org.proxy.library.umkc.edu/10.1080/0361526X.2021.1875958

Maceli, M. G. (2018). Encouraging patron adoption of privacy-protection technologies: Challenges for public libraries. *IFLA Journal*, *44*(3), 195–202. https://doi-org.proxy.library.umkc.edu/10.1177/0340035218773786

Maceli, M. G. (2019). Librarians' mental models and use of privacy-protection technologies. *Journal of Intellectual Freedom & Privacy*, *4*(1), 18–32. https://doi-org.emporiastate.idm.oclc.org/10.5860/jifp.v4i1.6907

Marden, B., & Cram, G. (2019). Privacy in public libraries. *Research Library Issues*, *297*, 38–46. https://doi-org.proxy.library.umkc.edu/10.29242/rli.297.4

Pedley, P. (2017). What can librarians do to protect user privacy? *Multimedia Information & Technology*, *43*(1), 20–24.

Rubel, A. (2014). Libraries, electronic resources, and privacy: The case for positive intellectual freedom. *Library Quarterly*, *84*(2), 183–208. https://doi-org.proxy.library.umkc.edu/10.1086/675331

Wu, Z., Xie, J., Pan, J., & Su, X. (2019). An effective approach for the protection of user privacy in a digital library. *Libri: International Journal of Libraries & Information Services*, *69*(4), 315–324. https://doi-org.proxy.library.umkc.edu/10.1515/libri-2018-0148