ARTICLE

Privacy Audit of Public Access Computers and Networks at a Public College Library

Katelyn Angell

ABSTRACT

In 2021, the assessment-data management librarian at Lehman College Library decided to conduct a privacy audit of the Library's public computers and networks. This audit comprised one of the Library's two annual formal assessments of resources and services. The American Library Association's (ALA) Library Privacy Checklist for Public Access Computers and Networks was selected to review 17 key items related to protecting user privacy and confidentiality. Faculty and staff from Circulation, Library Technology, and Online Learning identified 10 indicators needing work. Suggestions are provided for collaboratively resolving these issues and future steps are described to continuously maximize the online security of the campus community.

INTRODUCTION

Lehman College Library has a longstanding deep commitment to safeguarding the personal information of the College's students, faculty, and staff. The Library maintains an extensive collection of research guides offering resources for its librarians on all aspects related to patron privacy and confidentiality. Library units frequently collaborate to ensure optimal adherence to professional best practices.

In 2021, the assessment-data management librarian resolved to conduct a privacy audit of the Library's public access computers and networks during the 2021–2022 academic year. The audit served as one of the Library's two annual assessment projects. As one of the College's Administrative, Educational, and Student Support (AES) units, the Library selects and evaluates two resources or services every year, concluding with a detailed report. The reports are submitted to the Office of Assessment and are included within an extensive Institutional Effectiveness Assessment Report.

Privacy audits are "procedures to ensure that your organization's goals and promises of privacy and confidentiality are supported by its practices. As a result, they protect confidential information from abuse and the organization from liability and public relations problems."[1] They are an important assessment procedure that should be undertaken periodically to help minimize the collection, retention, and dissemination of data—sometimes sensitive in nature—associated with library users. The American Library Association (ALA) further explains the significance of upholding these values: "In their provision of services to library users, librarians have an ethical obligation, expressed in the *Code of Ethics of the American Library Association* and the *Library Bill of Rights*, to preserve users' right to privacy and to prevent any unauthorized use of user data."[2] Despite this importance, there are challenges facing librarians that confound procedures and protocols to optimize privacy protection. These include complex technologies and laws, lack of employee time to dedicate to these tasks, and a lack of advocacy or complaints from users.[3]

Katelyn Angell (Katelyn.Angell@gmail.com) is Medical Librarian at the City University of New York (CUNY) School of Medicine. © 2023.

https://doi.org/10.5860/ital.v42i3.16233

Public access networks and computers were selected for this audit due to their essentiality in safeguarding the information-seeking needs and practices of the Lehman College community while on campus. This was a particularly timely project due to the fact that students were returning to campus in droves following COVID-19 related closures and had a strong need for public computer access. Critical aspects of computer privacy identified by ALA are access to privacy policies, erasure of browser activity and personal data, protection from malware, and prevention of monitoring and tracking.

LITERATURE REVIEW

Privacy audits can be conducted on a wide range of resources and services within libraries. These areas include electronic resources vendors, integrated library systems, public networks and computers, assistive technology, and library websites. Magi urged fellow librarians to conduct privacy and confidentiality audits to guard the public trust as far back as 2006, specifying 12 potential areas.[4] These include records of websites visited and emails sent and received on library computers. ALA offers extensive checklists dedicated to assisting libraries and vendors in conforming to the Library Privacy Guidelines. These documents are products of ALA's Intellectual Freedom Committee.

Privacy audits are undertaken by academic libraries,[5] law libraries,[6] school libraries,[7] and public libraries.[8] Despite toolkits on conducting privacy audits from ALA and organizations like the Library Freedom Project, there is a major lack of scholarship on these compliance procedures within library and information science literature.[9] Public libraries provide the most freely available documentation, although most of this information is presented on a library website and not written up as scholarly articles. A prime example is San Jose Public Library, which offers a detailed account of a privacy audit across departments, including access services, technical services, marketing and communications, and security.[10]

Choosing not to conduct privacy audits can jeopardize the anonymity and security of library users. This concern is increasing in an era heavily impacted by the proliferation of big data and its ability to impose unprecedented surveillance. Marden warns of library users' information nonconsensually being bundled up and applied to "trend analyses, grant funding, and reporting to local governments."[11] Library users may not even be aware of these risks when sitting down at a computer to research, browse, or write, making it even more important for these security risks to be mitigated. In the days following the passage of the USA PATRIOT Act, which gave law enforcement agencies new powers to monitor patrons and obtain circulation records, Coyle suggested every library designate a "privacy officer."[12] This designee would stay abreast of privacy issues impacting the library and would oversee leading privacy audits and maintaining privacy policies.

A privacy audit is also useful because it plays an instrumental role in a library developing or revising a privacy policy.[13] It can reveal strengths and weaknesses in library policies and procedures and provide an opportunity for the staff to collectively devise more robust and current privacy protections. Currently, many academic and public libraries openly display patron data privacy policies on their websites. A particularly thorough and well-enumerated policy is that of MIT Libraries. Within the policy is the statement that the document is periodically reviewed by the Libraries and campus Audit Division.[14]

A privacy policy is just one way that librarians can help teach users how to take steps to best protect their data, especially on computers in public settings and/or with unsecured wireless connections. Key tenets of privacy literacy can be incorporated into critical thinking skill-building foregrounded in existing information literacy instruction sessions.[15] These skills can include online image management, achieved in part by carefully evaluating information prior to posting on social media sites.

Currently, there is very little scholarship exploring the application of the ALA Privacy Guidelines and Checklists within library and information science literature. The author hopes that this article can play a role in helping to increase the proliferation of privacy audits at academic libraries and, therefore, avoid online threats including identity theft, tracking/spying, and phishing.

METHODS

This study was conducted at Lehman College, a medium-sized urban college (about 15,000 students) in The Bronx, New York. Lehman is one of the 25 colleges within the City University of New York (CUNY) system. The Library does not have its own designated patron privacy policy; we default to a systemwide privacy policy.[16]

ALA's Library Privacy Checklist for Public Access Computers and Networks was used as the evaluation tool in this audit.[17] The checklist was employed in conjunction with ALA's Library Privacy Guidelines for Public Access Computers and Networks to determine the level of personally identifiable information and data recorded by the Library's computers and devices.[18] These particular assessment resources were selected due to their development by the United States' premier library professional organization. The instruments are still relatively new, approved by ALA in 2017.

To allow for streamlined evaluation of the 17 checklist items by multiple Library employees, the assessment-data management librarian followed the lead of San Jose Public Library and transferred the information from the ALA website to a shared Google document. Columns were added next to each checklist item for status (Needs Work, Accomplished, N/A), department (IT, Access, Technical Services), and a notes section for key comments related to past, present, and future planning and/or implementation.

The checklist was sent to the library technology coordinator, the web services-online learning librarian, and the head of Access Services. They independently reviewed the checklist and evaluated the privacy items falling within their professional duties. The tool was also shared with the business librarian, a library privacy specialist, for her expert review. An image of the completed checklist is presented in figure 1.

RESULTS

Analysis of the 17 items by Library employees reveals that while the Library is in full compliance with some of the guidelines devised by ALA, there remain steps to be taken that can enhance privacy and confidentiality of patron information transactions on our computers and network. These six fully accomplished items (identified in fig. 1) will not be further discussed in this report, as the Library has already achieved these goals. One other item will not be evaluated ("configure any content filters to not collect or share browsing data"), as it has been determined to not be relevant to the Library's purposes.

Ten items flagged as needing work will be focused on for the remainder of the report, accompanied by evaluator notes and potential future steps.

Table 1. ALA Privacy Checklist for Public Access Computers and Networks applied to the Lehman College Library

ALA Checklist Item	Status	Department
Use analog signage and/or splash screens to explain the library's network and Wi-Fi access policies, including any privacy-related information.	Needs Work	Library Technology
Make a policy decision about the level of privacy versus convenience that the library will offer its Wi-Fi users and adequately warn users of potentials for traffic interception and other risks of an insecure network.	Needs Work	Administration (determined by author)
Set up public computers to purge downloads, saved files, browsing history, and other data from individual user sessions.	Needs Work	Library Technology
Ensure that paper sign-up sheets for public computers, devices, or classes are destroyed when no longer needed.	Accomplished	Access Services
Offer classes and other educational materials to users about best practices for privacy and security when using the library's public computers.	Needs Work	Reference and Instruction (determined by author)
Offer privacy screens to patrons who desire to use them.	Needs Work	Access Services
Use antivirus software on all public computers. Ensure that antivirus software that is installed has the ability to block spyware and keylogging software.	Accomplished	Library Technology
Ensure that any computer reservation management system records, print management records, or ILS records in regards to computer use are anonymized or destroyed when no longer needed.	Needs Work	Access Services
Configure any content filters to not collect or store browsing data.	N/A	Library Technology
Anonymize or destroy transactional logs for network activity when no longer needed.	Needs Work	Library Technology
Perform regular security audits on all public computers, including digital inspection of security risks and flaws and physical inspection for unknown devices.	Needs Work	Library Technology
Install plugins on public computers to limit third-party tracking, enable private browsing modes, and force HTTPS connections.	Accomplished	Library Technology
Install the Tor browser on public computers as a privacy option for patrons.	Needs Work	Library Technology
Offer the privacy-oriented Tails OS on bootable USB or CDROM for use on public computers or patron devices.	Needs Work	Library Technology
Install malware-blocking, ad blocking, and anti-spam features on firewalls.	Accomplished	Library Technology
Segment the network to isolate staff computers, public computers, and wireless users into their own subnets.	Accomplished	Library Technology
Ensure that any applications and operating systems on public computers are disabled from automatically sharing activity data with software publishers (e.g., error reporting).	Accomplished	Library Technology

DISCUSSION

After careful study of numerous library privacy websites and reviews of existing literature on privacy within library science literature, combined with the useful appraisal of the three evaluators, the assessment-data management librarian devised recommendations for the increased safeguarding of privacy and confidentiality for Library patrons.

These recommendations are provided in tandem with the recognition that Library staff already provide the campus community with ample privacy protections. It is important to acknowledge that ALA's guidelines function within the understanding that not every library can accomplish every item or priority on the checklist due to factors related to technical expertise, resources/funding, and organizational structure.

The 10 priorities noted by the evaluators as needing work are listed in table 2, accompanied by a perceived barrier (when relevant) and recommendation for a potential solution. The generation of the barriers and recommendations was and will remain a collective effort across Library units. Additional recommendations for the priorities were solicited for this project from library and information sciences scholarship.

Table 2. Recommendations for accomplishing outstanding tasks related to privacy within public computers and networks.

Item Needing Work	Perceived Barrier	Recommendation
Use analog signage and/or splash screens to explain the Library's network and Wi-Fi access policies, including any privacy-related information.	Only Campus IT, not Library, can presently update analog signage in building.	Campus IT and Access Services can collaborate to facilitate access.
Make a policy decision about the level of privacy versus convenience that the Library will offer its Wi-Fi users.	Decision is not articulated as an official policy.	Co-author a Library-level policy balancing privacy level and convenience. Post on the Library website and near public computers. Hennepin Library Patron Data Privacy Policy provides a strong template.
Set up public computers to purge downloads, saved files, browsing history, and other data from individual user sessions.	Library Technology staff time (will have to reconfigure the image used on all computers to accomplish this goal). Users who accidentally save to a computer's desktop or download files and return later to find their files and history wiped.	A script can be created and loaded on desktop which when chosen will delete content from locations specified within the script. Programming computers to auto wipe/reset overnight instead of wiping between user sessions.
Offer classes and other educational materials to users about best practices for privacy and security when using the Library's public computers.	Lack of personnel time and resources.	Add key external information on these topics to research guides and share with patrons during library instruction classes and reference transactions.

Item Needing Work	Perceived Barrier	Recommendation
Offer privacy screens to patrons who desire to use them.	Uncommon request.	Purchase 1–2 screens and store; do not offer but provide upon direct request by patron.
Ensure computer reservation management system records, print management records, or ILS records in regard to computer use are anonymized or destroyed when no longer needed.	LibCal reservations are required for students to reserve group study rooms (at time of evaluation, individual reservations were required to visit Library due to COVID-19).	Keep user information two weeks after LibCal reservation is made for COVID-19 tracing purposes, but purge contact information after two weeks.*
Perform regular security audits on all public computers, including digital inspection of security risks and flaws and physical inspection for unknown devices.	Time/resources.	Campus IT Networking Group can work on accomplishing this objective.
Anonymize or destroy transactional logs for network activity when no longer needed.	This priority is N/A regarding virtual desktop implementation for units in the Education Library. Desktops and Macs across Library building need work.	Campus IT Networking Group can work on accomplishing this objective.
Install Tor browser on public computers as privacy option for patrons.	Browser hasn't been previously installed.	Library Technology staff note they can install browser onto public computers. Encourage students to use DuckDuckGo as their browser in lieu of Google, as it is committed to protecting online privacy.
Offer the privacy-oriented Tails OS on bootable USB or CD-ROM for use on public computers or patron devices.	Booting off a USB drive is an option but requires elevated rights.	Adding a password in BIOS will prevent users from using bootable USBs or CD-ROMs.

*August 2022 update: Library visit booking information for last year was purged when the Circulation unit made changes to visit criteria 1 hour/2 hour/day pass.

The ability to accomplish the aforementioned tasks is contingent on continued close collaboration between Library employees. While conducting the audit and writing this report is an important step in maintaining data privacy, it remains a work in progress. The assessment-data management librarian recommends formation of a task force to focus on achieving as many of these tasks deemed realistic given existing financial and personnel circumstances.

Duke Libraries describe development of a data privacy task force.[19] Its main duties are to "review the Audit report and gather any additional data necessary to inform their work, which may include setting priorities, working with departments and units to create policies where they are lacking, making recommendations for how to communicate policies to patrons, and other tasks determined by the task force." The Library's task force could meet on a semester basis to reflect on the status of data privacy protections and reassess if interventions are functioning efficiently or require modification.

Further research reveals additional steps taken by external libraries to enhance online privacy protocols. Robinson began using the free certificate program Let's Encrypt for library servers and services at the University of Alaska.[20] He provides instructions for employing the program to an API server. In addition, an extensive privacy audit at San Jose Public Library resulted in a detailed action plan.[21] Relevant items included developing a library data breach policy and installing research tracking plugins like Privacy Badger on public computers to prevent collection of user data by unwanted third parties.

ALA's Library Privacy Policies Report details an analysis of over 100 American academic and public library privacy policies.[22] This document offers extensive information on how a wide selection of libraries attempt to best protect patron privacy regarding data collection, third-party platforms, data security, and data retention. The report lists specific examples of text culled directly from library privacy policies, some of which pertain directly to material on ALA checklists and can be used to better safeguard privacy and confidentiality at this Library. For example, Rutgers University Libraries assures users that they "remove cookies, web history, cached files, or other computer and Internet use records and other software code that is placed on our public computers or networks after each use." This author maintains that all policies should include a recommendation to use DuckDuckGo for web browsing, as well as the posting of signs with this recommendation in public computer areas. In general, DuckDuckGo is as efficient in resolving information queries as Google and does not store or track search history.[23] The lack of targeted ads on DuckDuck Go, for example, shows the level of privacy that can be maintained while using the browser.

Lastly, the assessment-data management librarian suggests sharing this report with the University Library System's Privacy Roundtable. The Roundtable could review these findings and contribute recommendations from experiences at their own libraries, thus potentially improving data security and confidentiality for both the College community and other campuses within the university system. This is particularly important as students, faculty, and staff in the system are free to use libraries at any of the campuses (except for the law school).

CONCLUSION

There are a few limits of this privacy audit worth mentioning. First, the assessment was conducted during the COVID-19 pandemic within a hybrid remote/in-person working and learning environment. Employees and patrons alike were on campus part time, leading to far less computer and network usage than in previous years.

A related limitation is that evaluation with the ALA Checklist was conducted by each library participant separately over email, not as a group working in tandem in real time. A future study could benefit from the audit occurring in person, with each individual able to observe and assess existing conditions together in relevant library spaces.

Another limit is that this project was spearheaded by the assessment-data management librarian, who does not possess a professional background in information technology and library systems. While this librarian had ample support and assistance from colleagues during the audit and writing of this report, her own direct knowledge of public computing and networks can be considered a weakness. This limit reiterates the necessity of interdepartmental collaboration on running privacy audits and successfully applying fixes identified during the process.

To capably implement the priorities determined as needing work, it would be optimal to create a combined Library Data Privacy Task Force. The most critical aspect of an audit, as argued by Matz, is that it is "only an initial assessment, because a privacy audit should be an ongoing process for the library and its staff."[24] Encroachment on online privacy by not just scammers or other malicious parties, but companies we often know and trust, does not require a one-time fix. The latter has been reported to include Facebook, Zoom, WhatsApp, and Google.[25]

An analysis of public computers and networks is only one of many types of privacy audits that libraries can conduct. ALA has done an excellent service for the library profession by devising and sharing their Library Privacy Checklists. Future studies within academic library scholarship can explore audits of different key aspects of information security, such as assistive technology, vendors, and integrated library systems. By conducting these studies and sharing our findings with the greater community, we as a profession can collectively greater protect user data.

ACKNOWLEDGEMENTS

I would like to thank the following Lehman College colleagues for their assistance and support throughout this project: John DeLooper, Raymond Diaz, Martha Lerski, and Stephen Walker.

ENDNOTES

[1] American Library Association, "Privacy Audits," October 2021, https://www.ala.org/advocacy/privacy/audits#:~:text=Privacy%20audits%20are%20procedures%20to,liability%20and%20public%20relations%20problems.

[2] American Library Association, "Library Privacy Guidelines for Vendors," January 2020, https://www.ala.org/advocacy/privacy/guidelines/vendors.

[3] Tucker Taylor, "Library Privacy 101," November 2018, https://www.scla.org/assets/docs/2018_Conference/Library%20Privacy%20101.pptx.

[4] Trina J. Magi, "Protecting Library Patron Confidentiality: Checklist of Best Practices," *Illinois Library Association* (Fall 2006), https://www.ila.org/advocacy/making-your-case/privacy/confidentiality-best-practices.

[5] Margaret Heller, "Creating a Privacy Policy from the Ground Up," *ACRL Tech Connect* (February 2018), https://acrl.ala.org/techconnect/post/creating-a-privacy-policy-from-the-ground-up/; Patrick O'Brien et al., "Protecting Privacy on the Web: A Study of HTTPS and Google Analytics Implementation in Academic Library Websites," *Online Information Review* 42, no. 6 (2018): 734–51, https://doi.org/10.1108/OIR-02-2018-0056.

[6] Rachel Gordon, "Privacy Audits in the Law Library," July 2014, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2461235.

[7] Donna Riehl, "Students' Privacy Rights in School Libraries: Balancing Principles, Ethics and Practices," *School Libraries in Canada* 26, no. 2 (2006), http://accessola2.com/SLIC-Site/slic/262studentsprivacyrights.html.

[8] San Francisco Public Library (SFPL), "SFPL Data Privacy Audit," accessed February 2, 2023, https://sfpl.org/about-us/sfpl-data-privacy-audit; Erin Berman and Julie Oborny, "A Practical Guide to Privacy Audits," YouTube video, 2018, 55:55, https://www.youtube.com/watch?v=aq5upxSSkOk.

[9] Library Freedom Project, "Privacy Toolkit for Librarians," May 2017, https://libraryfreedom.org/privacy-toolkit-for-librarians/.

[10] San Jose Public Library (SJPL), "Privacy Audit," accessed February 1, 2023, https://www.sjpl.org/privacy/privacy-audit.

[11] William Marden, "Choose Privacy Week 2018: Big Data is Watching You," *Journal of Intellectual Freedom & Privacy* 4, no. 1 (2019): 3–4, https://doi.org/10.5860/jifp.v4i1.6885.

[12] Karen Coyle, "Make Sure You Are Privacy Literate," *Library Journal* 127, no. 16 (October 2002): 55–57, http://www.kcoyle.net/privacy_lj2.html.

[13] Shandra Morehouse et al., "Creating a Library Privacy Policy by Focusing on Patron Interactions," in *Sustainable Digital Communities*, eds. Anneli Sundqvist et al. (Cham: Springer, 2020).

[14] MIT Libraries, "MIT Libraries Patron Data Privacy Policy," November 2020, https://libraries.mit.edu/about/policies/privacy-policy/.

[15] Christina L. Wissinger, "Privacy Literacy: From Theory to Practice," *Communications in Information Literacy* 11, no. 2 (2017): 378–89, https://files.eric.ed.gov/fulltext/EJ1166461.pdf.

[16] CUNY Libraries, "CUNY Libraries' Privacy Statement," January 2019, https://www.cuny.edu/about/administration/offices/library-services/policies/patron-privacy/.

[17] American Library Association, "Library Privacy Checklist for Public Access Computers and Networks," January 2020, https://www.ala.org/advocacy/privacy/checklists/public-access-computer.

[18] American Library Association, "Library Privacy Guidelines for Public Access Computers and Networks," January 2020, https://www.ala.org/advocacy/privacy/guidelines/public-access-computer.

[19] Joyce Chapman and Angela Zoss, "Duke Libraries Data Privacy and Retention Audit Report," January 2020, https://dukespace.lib.duke.edu/dspace/bitstream/handle/10161/20061/DUL%20Data%20Privacy%20and%20Retention%20Audit%202020%20-%20PUBLIC.pdf?sequence=1&isAllowed=y.

[20] Mike Robinson, "Let's Encrypt on an API Server," *Choose Privacy Everyday*, 2018, https://chooseprivacyeveryday.org/resources/https-lets-encrypt/recipe-for-lets-encrypt-on-an-api-server/.

[21] San Jose Public Library (SJPL), "Privacy Audit."

[22] Jason Vaughan, "Library Privacy Policies," *Library Technology Reports* 56, no. 6 (2020): 1–53, https://journals.ala.org/index.php/ltr/issue/viewFile/771/537.

[23] James Temperton, "I Ditched Google for DuckDuckGo. Here's Why You Should Too," *Wired* (November 2019), https://www.wired.co.uk/article/duckduckgo-google-alternative-search-privacy.

[24] Chris Matz, "Libraries and the USA Patriot Act: Values in Conflict," *Journal of Library Administration* 47, no. 3/4 (2008): 69–87, https://doi.org/10.1080/01930820802186399.

[25] Kayla Matthews, "6 Examples of Online Privacy Violation," *Cybernews* (September 2021), https://cybernews.com/privacy/6-examples-of-online-privacy-violation/.