Privacy Policy Implementation in North Carolina Public Libraries

Lucy Butcher

Master of Library and Information Science (MLIS)
University of North Carolina at Greensboro

December 2017

Abstract

This study examines how public libraries across North Carolina communicate with their patrons about privacy through the use of online privacy policies. It is hypothesized that most libraries offer their users a standardized privacy policy that highlights state privacy laws governing library records, but does not adhere to the detailed privacy policy standards suggested by the American Library Association. To determine whether this is the case, this study surveys 25 randomly selected public libraries from across the state to assess whether or not each library has a privacy policy posted on their website and the extent to which that policy meets the criteria put forth by the ALA. The results show that the majority of public libraries surveyed do not have a privacy policy available on their website, and those that do are lacking in several key areas. The report then suggests a number of approaches to improve both privacy training and the implementation of more robust privacy policies in libraries across the state.

Table of Contents

Introduction....3

Literature review....4

Background....4

ALA privacy policy standards....4

Legal considerations....6

An even more rigorous approach....6

Privacy policies in practice....7

Research methods....9

Hypothesis....9

Methodology....9

Results....11

Conclusions....17

Analysis....17

Charlotte Mecklenburg Library....17

Braswell Memorial Library....18

Standardized policies....18

Research flaws....18

Moving forward....20

Training....20

Privacy policy toolkit....20

Works Cited....22

Appendix A: Sample Privacy Policies....24

Introduction

Since the adoption of the Library Bill of Rights in 1939, the American Library Association has considered protecting patron privacy and confidentiality to be a bedrock component of the library's duty to promote intellectual freedom. The ALA Code of Ethics enshrines privacy as a key guiding principle for the profession, stating: "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" ("Code of Ethics of the American Library Association").

While librarians have been on the front lines of privacy advocacy for decades, the introduction of new technologies into the library has created challenges to carrying out this ethic in practice that have not yet been fully resolved. Although the ALA offers extensive guidelines and toolkits to help librarians tackle privacy issues related to emerging technologies, libraries have been relatively slow to implement some of these policies. This is understandable given the scope of the issue and the fact that many of the tools that most compromise patrons' privacy rights are also vital to libraries' ability to provide exceptional service to all users, the very first principle enumerated in the ALA's Code of Ethics. As librarians work towards the best possible solution to this tension between service and privacy, one aspect of patron privacy rights can be easily addressed: patrons' right to be informed about what policies govern the collection and storage of their personal information.

This study examines how public libraries across North Carolina communicate with their users about privacy in the library by randomly sampling 25 libraries from across the state to see whether they have a privacy policy posted on their website, how easy that policy is to locate and understand, and the extent to which that policy meets ALA standards as well as the more extensive criteria put forth by the ALA's Library and Information Technology Association. Through this research, I hope to reveal pain points and gaps in how public libraries inform users about privacy, with the goal of creating an advocacy project to help librarians better inform patrons about their rights. While libraries may never be able to offer patrons absolute privacy in an age where so much data is created and stored about users, communicating transparently about the library's privacy policies can give patrons the tools to make well-informed decisions about what risks they're willing to take with their information.

Literature review

Background

The ALA defines privacy as "the right to open inquiry without having the subject of one's interest examined or scrutinized by others" ("Privacy: An Interpretation of the Library Bill of Rights"). This right is considered to be implicit in Article IV of the Library Bill of Rights, which guarantees library patrons free access to ideas. Privacy in the library allows users to securely look up any kind of information without worrying about surveillance or judgment, while a lack of privacy has a chilling effect on free inquiry, discouraging patrons from searching for potentially controversial material out of fear or embarrassment due to the knowledge that someone might be watching. In addition to suppressing inquiry, privacy violations of personally identifiable library data can also be dangerous for users, especially people who belong to marginalized groups, which are more visible in large datasets (Asher 49; Singer).

In addition to having a right to have their information protected, library patrons also have the right to be informed about their private information. In "Privacy: An Interpretation of the Library Bill of Rights," the ALA states that one of the privacy rights of library users, alongside the right to be free from intrusion or surveillance of any kind, is the "right to be informed" about how the library deals with personally identifiable user information and what the patron can do to maintain his or her privacy ("Privacy: An Interpretation of the Library Bill of Rights"). By this standard, libraries have an ethical responsibility not only to securely protect patrons' records, but also to communicate to users how their data is being collected and why.

The need for libraries to be transparent about privacy becomes even more urgent in light of the myriad ways in which a patron's privacy can be compromised online, from third-party vendor services that are not governed by the same privacy laws as libraries, to unsecured library websites, to ebook services, to social media, to web analytics tracking, and many more services that create and collect data about library users. Many of the most potentially problematic tools are also the most useful to librarians; every library needs a dynamic web page, a social media presence, data about website users, and so on, in order to provide excellent service to their patrons.

The ALA advises that libraries address these potential vulnerabilities by limiting the degree to which the library and third-party service providers collect and share personally identifiable user data, avoiding creating unnecessary records, avoiding retaining records that are not absolutely necessary for the operation of the library, avoiding practices that place personally identifiable information in public view, and storing patron records on a local server rather than the cloud or a third-party server. The ALA also urges libraries to craft a publicly available, easy-to-read privacy policy that details these practices ("Developing or Revising a Library Privacy Policy").

ALA privacy policy standards

According to the ALA, "a well-defined privacy policy tells library users how their information is utilized and explains the circumstances under which personally identifiable information might be disclosed" ("Developing or Revising a Library Privacy Policy"). Beverley Becker in the Office for Intellectual Freedom's *Intellectual Freedom Manual* argues that putting detailed policies into writing in this manner is important because it reduces confusion about

procedures, gives credence to the library's actions, informs the community about the library's practices, gives the public a means to evaluate the library's performance, disarms potential critics, and offers evidence of the library's normal practices (Becker 417).

In its library privacy toolkit, the ALA offers guidelines for how to develop a standard privacy policy that achieves these goals. Importantly, the ALA suggests that before setting out to craft a privacy policy, a library should first perform a privacy audit to discern where the library collects personally identifiable information. After completing this audit, the ALA advises that the library draft a privacy policy written in accessible language that covers the following issues:

- **Notice & Openness:** The privacy policy should explain patrons' right to privacy and confidentiality in the library, and what policies the library has implemented to protect their information. This section should include an explanation of what kinds of user data the library collects and for what purposes, where and for how long this information is stored, who has access to it, under what conditions it can be shared, and how it is used by the library and others.

- **Choice & Consent:** The library should give users as much choice as possible in regard to how their personally identifiable information is collected and used. While some data collection is unavoidable in order to effectively run the library, patrons should be given the chance to opt out of any secondary services that collect information (or, ideally, should be required to affirmatively opt in to these services). The library should "retain this information only as long as is necessary to fulfill the function for which it was initially required" ("Developing or Revising a Library Privacy Policy").

- **Access by Users:** The ALA notes that users "have the right to access their own personally identifiable information," and that a library's privacy policy should notify patrons of this right and explain how users can access their information onsite or securely online ("Developing or Revising a Library Privacy Policy").

- **Emerging Technologies with Privacy Concerns:** The ALA states that it is "imperative that libraries understand each new technology by defining them and identifying the mechanism through which each patron's privacy may be breached" ("Developing or Revising a Library Privacy Policy"). This includes but is not limited to privacy vulnerabilities in library apps, camera surveillance, cloud computing, ebook services that track users' digital reading habits, OPACs that may have different privacy policies from those of the library, RFID technology, social networking tools, and more. The library should make sure that patrons understand the possible vulnerabilities involved in using these technologies so that the patron can make an informed decision about what risks they're willing to take.

- **Data Integrity & Security:** The library should communicate how it ensures data integrity. Examples of this include destroying outdated personally identifiable information, encrypting stored data, stripping personal identifiers from aggregated data, and using proper security protocols. If the library uses cookies, it should

instruct users how to refuse and delete them. The library should also advise users about the security limitations involved in using third-party services.

- **Enforcement & Redress:** The library should maintain effective mechanisms to enforce its privacy policies, and should offer users a system for redress if they feel that their privacy or confidentiality rights have been violated. The library should also educate users about how to protect their privacy both within and outside of the library.

- **Government Requests for Library Records:** The library should inform users about the conditions under which the library might be legally required to release personally identifiable information to law enforcement.

Legal considerations

In addition to professional ethics, the ALA instructs libraries to review their privacy policies to make sure they are in compliance with any applicable laws.

The right to privacy in the United States stems from Samuel Warren and Louis Brandeis's 1890 essay "The Right to Privacy," in which they defined privacy as "the right to be let alone" (Warren and Brandeis 193). Common law privacy protections have expanded the definition of privacy over the past century, culminating with a series of Supreme Court decisions in the 1960s and '70s that recognized privacy as a constitutional right. A number of federal and state laws have further increased legal privacy protections, including in regard to library patron records (Givens 347).

Chapter 125, Article 3 of the North Carolina General Statutes states that "a library shall not disclose any library record that identifies a person as having requested or obtained specific materials, information, or services, or as otherwise having used the library, except as provided for in subsection (b)," where subsection (b) includes the following exceptions:

1. When necessary for the reasonable operation of the library;
2. Upon written consent of the user; or
3. Pursuant to subpoena, court order, or where otherwise required by law. (G.S. 125-18)

An even more rigorous approach

In *Protecting Patron Privacy: A LITA Guide,* Andrew Asher argues for an even more stringent approach to drafting privacy policies than that proposed by the American Library Association. Asher suggests that the tension between providing the best possible service and protecting patron privacy should be dealt with by applying the ethical framework of human subjects research to the assessment of library data collection practices. While Asher discusses this model in reference to academic libraries, his perspective is also useful in the context of public libraries.

Scientific research involving human subjects is regulated by Institutional Review Boards charged with ensuring that a researcher's methods meet three guiding principles for the protection of their subjects: respect for persons, beneficence, and justice. The principle of respect for persons ensures that research subjects are treated as autonomous agents, and that people with diminished autonomy are protected from activities that might cause them harm. This principle

establishes the necessity of informed and voluntary consent as a prerequisite for participating in research. The principle of beneficence calls on researchers to do no harm, and to maximize possible benefits for participants and minimize possible risks. Finally, the principle of justice requires equitable selection of research subjects (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research).

In the context of human subjects research, limiting the collection, sharing, and retention of unnecessary personally identifiable information becomes a matter of not only protecting privacy rights, but also of respecting an individual's autonomy and making every effort to prevent potential harm. Moreover, under this ethical framework, simply making a privacy policy publicly available isn't enough to qualify as obtaining fully informed consent from a patron. Asher writes:

> Libraries routinely obtain passive consent for user-data collection through mechanisms such as by posting a library privacy policy. These policies are sometimes out of date or incomplete, or do not adequately and fully explain what data is collected, how it will be used, and what other data it might be linked to. These types of policies are an insufficient consent instrument from a research perspective not only for these reasons, but also because they are not widely read or understood by library users. (Asher 48)

The typical library privacy policy also falls short on this front because most do not offer users a practical way to opt out of data collection. Asher argues that the manner in which data collection is built into library systems means that there is only one effective way for patrons to opt out: by not using the library. This, he contends, turns using the library into a coercive situation in which users are not able to offer fully voluntary consent.

On the principle of justice, Asher makes the troubling point that "minority groups of any type [...] will always be more visible within a systematically collected dataset, and by extension, individual members of these groups will be easier to potentially identify" (Asher 49). Even when aggregate data has been de-identified, he points out, it's often easier than one might expect to reconnect the dots and match datasets back to their creators (Asher 51). This highlights even further the need for libraries to avoid unnecessary data collection.

While it may not be possible for libraries to fully adhere to human subjects research standards, Asher offers some practical steps that can be taken to move closer to this goal. First, he argues that libraries should seek explicit consent and use opt-in models for data collection whenever possible, rather than relying on passive consent and users opting out of services. Second, he suggests that data security procedures should assume that user information will eventually be compromised, and prepare accordingly by taking preventative measures like "physically separating subject identification data from analysis datasets" (Asher 50). Finally, Asher contends that datasets containing personally identifiable information should be thought of as toxic assets and destroyed accordingly whenever possible (Asher 51).

Privacy policies in practice

What does an ethical and robust library privacy policy look like in practice? Many libraries have excellent, user-friendly privacy policies that fully meet ALA standards. A particularly standout example is that of the New York Public Library. Their privacy policy is

unique not only because it's very well crafted, but also because the library has documented in detail the processes they undertook in order to revise it.

NYPL Director of Privacy and Compliance William Marden writes that completing a privacy audit and learning about the library's processes for collecting and storing patron information "was a whole-scale effort that involved speaking with every department in the library to better understand the reasons for collecting the data" (Marden). It took the library four months to draft and roll out a new policy, a timeline that demonstrates the level of intensive work required to produce a policy that meets the ALA's ethical standards.

The NYPL's new and improved privacy policy is easy to locate on the library website. It is written in clear, simple terms, and is available in English, Spanish, Chinese, and Russian. The policy informs users about both state law and the library's ethical commitment to protecting patron privacy, and gives a detailed breakdown of how user information is collected directly, indirectly, and through cookies. It offers users multiple processes by which to access and update or delete personal information stored by the library, instructs users how to remove or reject the library's cookies, and assures users that information collected by these means is de-identified and aggregated for security purposes.

The policy further explains to users how their information is utilized by the library, including to issue library cards, to deliver personalized services, to provide access to ebooks, to administer promotions, and to remember the user's website preferences, and also gives users a detailed breakdown of when personal data stored by the library can be shared. This includes when users share content through the library's online services, when users engage with third-party library service providers, as part of fundraising and marketing outreach, in response to legal requests, and when the library reports financial contributions.

Importantly, after the policy was implemented, the NYPL made a committed effort to publicize the new policy through both a feature on the main website and email marketing to users.

The policy can be read in full here: www.nypl.org/help/about-nypl/legal-notices/privacy-policy

A longer list of sample library privacy policies that meet ALA standards can be found in Appendix A.

Research methods

Hypothesis

I began this study with a hypothesis that most North Carolina public libraries would offer a standard, boilerplate privacy policy on their website. I theorized that most of these policies would cite applicable state privacy laws and make a general statement regarding the library's dedication to protecting patron privacy, but that most would lack more specific details regarding privacy vulnerabilities related to emerging technologies. I expected that a handful of libraries would not have a privacy policy posted, and also that a handful would have better-than-average privacy policies.

Methodology

In order to conduct my research, I first randomly selected 25 county public library systems and municipal public libraries from the State Library of North Carolina's Directory of Public Libraries. I assigned each library in the directory a number, and then used a random integer generator to randomly select 25 libraries to survey. I chose to focus on county and city libraries rather than individual library branches because most branches do not have their own separate policies or websites, but are rather represented by their larger library system.

I next surveyed these 25 library websites to assess whether or not each library had a publicly available privacy policy and the extent to which that policy met the standards suggested by the ALA and LITA. I broke these criteria down into the following series of questions:

1. Is there a privacy policy available on the website?
2. Is the policy easy to find?
3. Is it written at an accessible reading level?
4. Is it available in multiple languages?
5. Does the policy include a notification of patrons' right to privacy? Does it explain what policies the library has implemented to protect this right?
6. Is the definition of personally identifiable information explained clearly?
7. Does the policy explain what type of data is collected by the library and why?
8. Does the policy explain when patron data can be shared and under what conditions?
9. Does the policy advise users of security limitations involved in visiting third-party sites?
10. Does the policy instruct users how they can access their personal information?
11. Does the policy offer appropriate opt-out or opt-in methods for user consent?
12. Does the policy cover specific privacy issues related to emerging technologies?
13. Does the policy explain how personal information is stored and secured by the library?
14. Does it include a schedule for when personal information is deleted?
15. Is there contact information listed, a way for users to seek redress or ask questions?
16. Does the policy include a description of applicable privacy laws?

Questions 4 and 6 were not explicitly referenced by the ALA or LITA, but I felt they were important to include in order to accomplish Andrew Asher's ideal of a privacy policy that obtains fully informed consent from users, as a patron cannot fully consent if they cannot read the policy because it's written in a language they do not speak, or if they do not understand the basic definition of what constitutes personally identifiable information.

Finally, if a library did not have a privacy policy posted publicly on their website, I sent a follow-up email inquiring about whether or not a policy was available in some other format, to ensure that I did not overlook policies that might be shared onsite in the library rather than online.

Results

	Alamance County Public Libraries	BHM Regional Library	Braswell Memorial Library	Brunswick County Library	Buncombe County Public Libraries
Privacy policy on website	No	No	Yes; not comprehensive	No	No
Link to policy			http://braswell-library.libguides.com/ld.php?content_id=25189495		
Easy to find?			Yes		
Easy to read?			Yes		
Multiple languages?			No		
Privacy right?			No		
PII defined?			No		
Type of data collected and why?			Yes		
Data sharing policy?			Yes		
3rd party limitations?			Yes		
Access?			No		
Opt in/out?			No		
Emerging tech?			Yes, but only re: website		
How data is stored & secured?			No		
When data is deleted?			No		
Contact info			Yes		
Privacy laws			No		
Follow-up	No response	Policy is not publicly available.		No response	Privacy included in staff training.

	Cabarrus County Public Library	Chapel Hill Public Library	Charlotte Mecklenburg Library	Davidson County Public Library	Durham County Library
Privacy policy on website	No	Yes	Yes	No	No
Link to policy		https://chapelhillpubliclibrary.org/about-chpl/policies/	https://www.cmlibrary.org/privacy-policy		
Easy to find?		Yes	Yes		
Easy to read?		Yes	Yes		
Multiple languages?		No	Google Translate		
Privacy right?		Yes	Yes		
PII defined?		No	Yes		
Type of data collected and why?		No	Yes		
Data sharing policy?		No	Yes		
3rd party limitations?		Yes	Yes		
Access?		No	No		
Opt in/out?		No	Opt out; new services only		
Emerging tech?		No	No		
How data is stored & secured?		No	No		
When data is deleted?		No	No		
Contact info		No	No		
Privacy laws		Yes	No		
Follow-up	No response			No response	No response

	Edgecombe County Memorial Library	Forsyth County Public Library	Greensboro Public Library	Harnett County Public Library	Madison County Public Library
Privacy policy on website	No	No	Yes	No	No
Link to policy			http://www.greensboro-nc.gov/index.aspx?page=789#Privacy Statement		
Easy to find?			Yes		
Easy to read?			No		
Multiple languages?			No		
Privacy right?			Yes		
PII defined?			No		
Type of data collected and why?			No		
Data sharing policy?			No		
3rd party limitations?			No		
Access?			No		
Opt in/out?			No		
Emerging tech?			No		
How data is stored & secured?			No		
When data is deleted?			No		
Contact info			No		
Privacy laws			Yes		
Follow-up	No response	No response		No response	No response

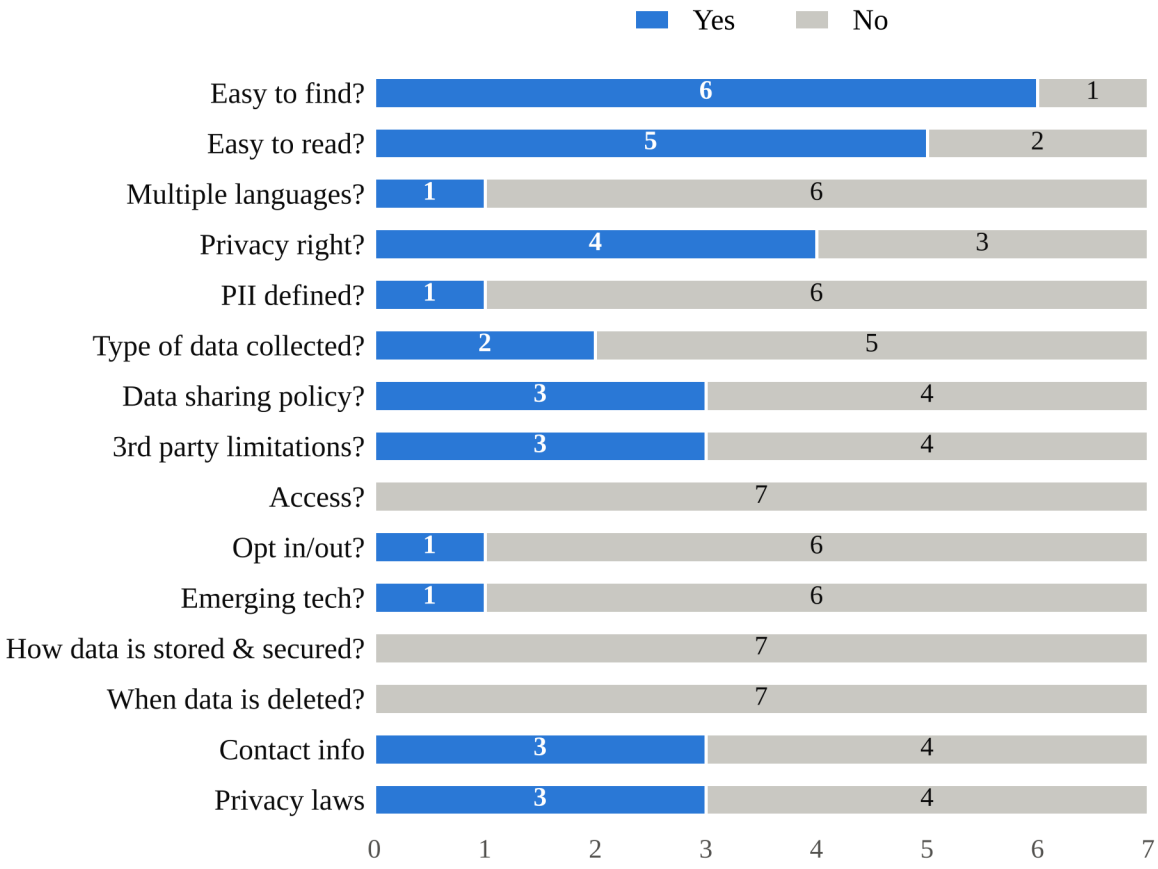
	Mauney Memorial Library	New Hanover County Public Library	Northwestern Regional Library	Onslow County Public Library	Public Library of Johnston County and Smithfield
Privacy policy on website	No	Yes	No	No	No
Link to policy		http://libguides.nhcgov.com/ld.php?content_id=8394309			
Easy to find?		No			
Easy to read?		No			
Multiple languages?		No			
Privacy right?		Yes			
PII defined?		No			
Type of data collected & why?		No			
Data sharing policy?		Yes			
3rd party limitations?		No			
Access?		No			
Opt in/out?		No			
Emerging tech?		No			
How data is stored & secured?		No			
When data is deleted?		No			
Contact info		No			
Privacy laws		Yes			
Follow-up	Confirmed no policy		No response	No response	Confirmed no policy, but that they follow state & fed law

	Randolph County Public Library	Sampson - Clinton Public Library	Stanly County Public Library	Wake County Public Libraries	Wilson County Public Library
Privacy policy on website	No	Limited records privacy policy	No	Limited email privacy policy	No
Link to policy		http://www.sampsonnc.com/document_center/Library/Privacy_of_Records_Policy___Copy.pdf		http://www.wakegov.com/libraries/services/about/Pages/emailpolicy.aspx	
Easy to find?		Yes		Yes	
Easy to read?		Yes		Yes	
Multiple languages?		No		No	
Privacy right?		No		No	
PII defined?		No		No	
Type of data collected & why?		No		Limited to email addresses	
Data sharing policy?		Only re: patron records		No	
3rd party limitations?		No		No	
Access?		No		No	
Opt in/out?		No		No	
Emerging tech?		No		No	
How data is stored & secured?		No		No	
When data is deleted?		No		No	
Contact info		Yes		Yes	
Privacy laws		No		No	
Follow-up	No response		No response		No response

The breakdown of libraries that had a publicly available privacy policy versus those that did not:



Among libraries that did have a privacy policy, the policies included the following assets:



Conclusions

Analysis

My study shows a far more extensive problem related to the implementation of privacy policies in North Carolina public libraries than I originally hypothesized. I predicted that most libraries would offer a standardized privacy policy that communicates the state law related to patron records and the library's dedication to protecting patron privacy, but perhaps offered no more detail beyond this. I assumed that the most important question would be related to the level of detail included in these policies, but my results indicate that instead the major issue may in fact be whether or not a privacy policy exists at all. Of the 25 libraries I surveyed, only 7 had a privacy policy available, just 28% of the total.

Of the libraries that did have a privacy policy available on their website, many exceeded my expectations; however, none met all of the ALA's standards for an ideal privacy policy, or the more rigorous criteria in *Protecting Patron Privacy: A LITA Guide.* Three of the privacy policy features I examined did not appear in any of the library privacy policies included in the survey: no library offered users access to their personal data, none explained how personally identifiable information is stored and secured at their library, and none offered their users a timeline for when personally identifiable information would be deleted. Beyond that, only one library defined what constitutes personally identifiable information, only one library offered access to their privacy policy in multiple languages, only two explained what type of personal data is collected by the library and why, only one offered users a limited ability to opt out of new services, and only one addressed privacy issues related to emerging technologies.

On the positive front, almost all the available privacy policies were easy to find and written at an accessible reading level, with the exception of one that was composed in dense legal language. A little more than half of the policies defined patrons' right to privacy in the library and the library's commitment to protecting this right. A little less than half explained their policies for when and under what conditions personal data might be shared with other parties, the privacy limitations of third-party websites, and what privacy laws apply to the library. Finally, three out of seven of the policies included information about how users could ask questions or register complaints.

Beyond this statistical breakdown, it's worth taking a moment to zoom in on some of the qualitative aspects of the policies surveyed, as a few of the privacy policies included unique sections that deserve further attention.

Charlotte Mecklenburg Library

The Charlotte Mecklenburg Library features the most detailed, comprehensive policy of all the libraries included in this survey. Its policy covers website data collection, registration and circulation records, photos posted on social media, online credit card transactions, and external links to third-party websites. It is the only library to specifically define what counts as personally identifiable information, the only library to explain what cookies are and when they will be deleted, and the only library to make their privacy policy available in multiple languages (albeit via a Google Translate plugin, which likely is not the ideal way to translate information that might have sensitive legal implications). Notably, Charlotte Mecklenburg is also the only library surveyed to offer a mechanism for users to opt out of any services. The library explains:

> From time to time, we may use visitor information for new unanticipated uses not previously disclosed in our privacy notice. If our information practices do change, we will post the policy changes on our site to notify you and provide you with the ability to opt out of these new uses. ("Charlotte Mecklenburg Library Privacy Policy")

The Charlotte Mecklenburg Library's privacy policy can be read in full here: https://www.cmlibrary.org/privacy-policy

Braswell Memorial Library

While not as comprehensive overall as Charlotte Mecklenburg's policy, the Braswell Memorial Library does the best job of all the libraries surveyed of clearly explaining the conditions under which their library makes patron data available to third-party services. For example, the library explains their use of Google Analytics as follows:

> The library uses services provided by Google Analytics to collect web site and online service usage statistics. To provide those services Google Analytics may collect information like Internet addresses, browser, and operating systems types, pages visited, referring web sites, types of searches conducted, and search terms used. The information collected is provided to the library for statistical purposes and may be used by Google Analytics for their statistical and marketing purposes. The privacy policies of Google Analytics would apply to those purposes. Names and email addresses of library customers are not collected or provided to Google Analytics. ("Braswell Memorial Public Library Website Privacy Policy")

While the Braswell Memorial Library's policy only covers data collected through the library website, rather than the library's full privacy policies, it gives users a clear understanding of how these web services collect user information and for what purpose.

The Braswell Memorial Library's privacy policy can be read in full here: http://braswell-library.libguides.com/ld.php?content_id=25189495

Standardized policies

The New Hanover County Public Library, the Chapel Hill Public Library, and the Greensboro Public Library had the privacy policies that most closely resembled what I hypothesized most libraries would provide. Each highlighted North Carolina state law and the library's dedication to upholding patron privacy, but offered little detail beyond that.

Research flaws

While my study offers a quantitative analysis of how many North Carolina public libraries have implemented privacy policies and what features those policies include, it does little to investigate *why* the current gaps in privacy policy implementation exist. If I had realized going into this research that so many of the libraries surveyed simply would not have a privacy policy available, I would have shifted my methods to better account for this absence. Is the general lack of privacy policies related to a lack of training regarding privacy rights in the library more broadly? Could the gap stem from a lack of technical expertise regarding how to address privacy issues related to emerging technologies? Or is it the result of a lack of time or funding to perform the work-intensive library-wide audits necessary to craft a comprehensive policy? A project with

a larger scope involving more qualitative follow-up interviews with all the libraries surveyed could perhaps have answered some of these questions, and in doing so helped to better pinpoint the best way to go about advocating for improvement.

Moving forward

In order to advocate for the implementation of robust privacy policies in public libraries across North Carolina, I suggest a project in collaboration with the North Carolina Library Association's Intellectual Freedom Committee to increase privacy-related training and provide resources to libraries across the state to more easily draft comprehensive policies.

Training

In order to more transparently educate patrons about privacy issues in the library, it's vital for library staff to have an in-depth understanding of both patron privacy rights and possible privacy vulnerabilities. The ALA has published numerous guidelines, checklists, and toolkits for libraries related to a wide variety of privacy issues, but these policies have not yet become universally institutionalized. For example, fewer than 50% of libraries currently use HTTPS to completely secure their websites, even though the ALA has partnered with Let's Encrypt to make server certificates available to libraries at no cost (Ford; "ALA's Office"). This gap in implementation leads me to believe that more can be done to raise awareness about these resources at the local level.

To amplify the ALA's privacy training initiatives, some state library associations and municipal library systems have created their own projects aimed at increasing privacy awareness within local libraries. This work is also being done more broadly by a few nonprofit organizations, most notably the Library Freedom Project, which recently received a $250,000 IMLS grant to train librarians from across the country to serve as privacy advocates in their own communities ("RE-95-17-0076-17"). As a very first step, before attempting to create an entirely new privacy training program, my project would engage some of these existing organizations to offer privacy workshops to representatives from libraries across the state, perhaps in conjunction with the ALA's annual Choose Privacy Week.

To take privacy training at the state level a step further, I suggest that privacy advocates work with the NCLA to found a state-level organization similar to Brooklyn's Data Privacy Project, though alternatively this is a project that could also be accomplished at the level of the individual library system. The Data Privacy Project aims to teach New York City library staff "how information travels and is shared online, what risks users commonly encounter online, and how libraries can better protect patron privacy" ("Introduction"). The organization has made its entire training curriculum available online for free to other libraries who wish to replicate their work, making it a particularly efficient model to use as a starting point. This project could potentially be funded through a grant from IMLS.

Importantly, increased training and resources for staff members related to broader privacy issues would also enable North Carolina librarians to offer better privacy-related programming and services to their patrons, which in turn would help to further ensure library users are better informed about their rights.

Privacy policy toolkit

In order to assist North Carolina public libraries with the more specific task of drafting a privacy policy document, the NCLA's Intellectual Freedom Committee could follow the example of the Vermont Library Association and make its own Intellectual Freedom Toolkit

available on the NCLA website ("Intellectual Freedom Toolkit"). The Vermont Library Association's toolkit includes links to ALA resources on internet filtering, censorship challenges, and developing a library privacy policy, as well as a number of sample policies for libraries to use as examples. While this step wouldn't involve the creation of new materials, it would highlight the ALA's existing resources and make them more easily accessible to librarians across the state.

I recommend that North Carolina's version of this project go a step further, and offer state libraries an extensive standardized template to use as a basis for their individual library privacy policies. To accomplish this, the North Carolina Intellectual Freedom Committee could survey libraries across the state to see which technologies are most commonly used in the library —for example, Google Analytics, ebook reader services, cookies, social media, payment services, etc.—and offer standardized language that explains to users the privacy implications of each of these services. While this template wouldn't free libraries from the obligation of performing an intensive library-wide privacy audit, it would give libraries a starting point from which to understand how to better communicate complicated technical issues to their patrons. The template would also include boilerplate language related to state privacy laws, the definition of personally identifiable information, security limitations related to third-party websites, and patrons' right to privacy, as these issues are fairly consistent from library to library. Each library could then edit the template as needed to serve their individual purposes.

While a shared template may not be as ideal a solution as the rigorous process undertaken by the New York Public Library, for example, it would at least provide a starting point that would make the task less daunting. Moreover, if a library chose to use the template as is, rather than customizing it with further information, it would provide more information to patrons than many public libraries across the state are currently offering. Additionally, having a partially completed policy as a starting point might cut into some of the time and financial burden related to drafting a privacy policy, which are likely significant roadblocks to implementation.

Finally, I suggest that after these steps have been taken, the NCLA proactively market these resources to North Carolina libraries, and those libraries in turn amplify updates to their privacy policies to their users. One interesting tactic that the Library Freedom Project has employed in its effort to encourage libraries to use HTTPS is an HTTPS pledge that libraries can sign to demonstrate their dedication to protecting patron privacy ("HTTPS Pledge"). Perhaps a similar method could be used locally for libraries to show off the work they're doing to move towards better privacy policies. These marketing efforts could be tied into promotions and programming during Choose Privacy Week, so that librarians and patrons alike can better understand the relevancy of privacy issues in the library.

Works Cited

"ALA's Office for Intellectual Freedom Announces Sponsorship of Let's Encrypt Initiative." *American Library Association*, 15 Sept. 2015, www.ala.org/news/press-releases/2015/09/alas-office-intellectual-freedom-announces-sponsorship-lets-encrypt.

Asher, Andrew. "Risks, Benefits, and User Privacy: Evaluating the Ethics of Library Data." *Protecting Patron Privacy: A LITA Guide*, edited by Bobbi Newman and Bonnie Tijerina, Rowman & Littlefield, 2017, pp. 43-56.

Becker, Beverley. "Essential Preparation." *Intellectual Freedom Manual*, edited by Trina Magi, ALA Editions, 2005, pp. 417-28.

"Braswell Memorial Public Library Website Privacy Policy." *Braswell Memorial Library*, 10 Aug. 2011, braswell-library.libguides.com/ld.php?content_id=25189495.

"Charlotte Mecklenburg Library Privacy Policy." *Charlotte Mecklenburg Library*, www.cmlibrary.org/privacy-policy.

"Code of Ethics of the American Library Association." *American Library Association*, 22 Jan. 2008, www.ala.org/advocacy/sites/ala.org.advocacy/files/content/proethics/codeofethics/Code%20of%20Ethics%20of%20the%20American%20Library%20Association.pdf.

"Developing or Revising a Library Privacy Policy." *American Library Association*, Apr. 2017, www.ala.org/advocacy/privacy/toolkit/policy.

Ford, Anne. "How to Protect Patrons' Digital Privacy." *American Libraries Magazine*, 21 Apr. 2017, americanlibrariesmagazine.org/2017/04/21/protect-patrons-digital-privacy/.

Givens, Cherie. "Information Privacy and Cybersecurity." *Information Services Today*, edited by Sandra Hirsh, Rowman & Littlefield, 2015, pp. 345-56.

G.S. 125-18. *North Carolina General Assembly*, www.ncga.state.nc.us/EnactedLegislation/Statutes/PDF/ByArticle/Chapter_125/Article_3.pdf.

"HTTPS Pledge." *Library Freedom Project*, libraryfreedomproject.org/https-pledge/.

"Intellectual Freedom Toolkit." *Vermont Library Association*, www.vermontlibraries.org/ifc/ift/.

"Introduction." *Data Privacy Project*, dataprivacyproject.org/about/.

Marden, William. "The Path to Creating a New Privacy Policy: NYPL's Story." *Intellectual Freedom Blog*, 1 May 2017, www.oif.ala.org/oif/?p=9660.

National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. *The Belmont Report*. U.S. Department of Health and Human Services, 18 Apr. 1979, www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html.

Newman, Bobbi, and Bonnie Tijerina, editors. *Protecting Patron Privacy: A LITA Guide*. Rowman & Littlefield, 2017.

"Privacy: An Interpretation of the Library Bill of Rights." *American Library Association*, 19 June 2002, www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy.

"RE-95-17-0076-17." *Institute of Museum and Library Services*, 2017, www.imls.gov/grants/awarded/re-95-17-0076-17.

Singer, Natasha. "With a Few Bits of Data, Researchers Identify 'Anonymous' People." *The New York Times*, 29 Jan. 2015, bits.blogs.nytimes.com/2015/01/29/with-a-few-bits-of-data-researchers-identify-anonymous-people/.

Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy." *Harvard Law Review*, vol. 4, no. 5, 15 Dec. 1890, pp. 193-220. *JSTOR*, www.jstor.org/stable/1321160.

Appendix A: Sample Privacy Policies

The following privacy policies are a selection of comprehensive policies that meet the ALA's standards for an ideal privacy policy document:

Appleton Public Library	Appleton, WI	http://www.apl.org/system/files/privacy13.pdf
Berkeley Public Library	Berkeley, CA	https://www.berkeleypubliclibrary.org/sites/default/files/files/inline/10_19_privacy_policy_2008_12_10.pdf
Denver Public Library	Denver, CO	https://www.denverlibrary.org/content/privacy-policy
Multnomah County Library	Portland, OR	https://multcolib.org/privacy-and-confidentiality-library-records
New York Public Library	New York, NY	https://www.nypl.org/help/about-nypl/legal-notices/privacy-policy
Ottawa Public Library	Ottawa, ON, CA	https://biblioottawalibrary.ca/en/privacy-statement
Seattle Public Library	Seattle, WA	http://www.spl.org/privacy/the-seattle-public-library-website-privacy-notice
Sherburne Memorial Library	Killington, VT	https://sherlib.wordpress.com/about-us/policies/privacyconfidentiality/
Toronto Public Library	Toronto, ON, CA	http://www.torontopubliclibrary.ca/terms-of-use/library-policies/access-to-information-protection-privacy-policy.jsp