Creating a Library Privacy Policy by Focusing on Patron Interactions

Shandra Morehouse(✉), Jessica Vitak, Mega Subramaniam,
and Yuting Liao

University of Maryland, College Park, MD 20742, USA
{shandra, jvitak, mmsubram, yliao598}@umd.edu

Abstract. As sensitive transactions continue to move online, public libraries are becoming a critical resource to patrons without access to the internet. This paper shares insights on how library staff negotiate privacy risks when working with patrons handling sensitive and private information. Based on findings from an analysis of library policies on technology use, as well as focus groups and participatory design sessions with library staff from around the United States, we categorize primary risks patrons face when using library computers to complete information tasks requiring submission of sensitive information, as well as how library staff navigate the tensions between their professional values and privacy concerns. We conclude the paper with a discussion of how these findings are informing our development of a framework that library staff can use to navigate privacy risks patrons face.

Keywords: Libraries · Information needs · Privacy · Security · Information policy

1 Introduction

For low-income neighborhoods in the United States, one of the most important resources public libraries offer is access to computers and the internet. Data suggests that low-income Americans are much less likely to have internet access at home and many only access the internet through their smartphone [1]. At the same time, forms and services (e.g., job applications, banking, healthcare) increasingly require online transactions. Therefore, public library staff who assist patrons using public computers play an important role in helping patrons get access to a variety of services to satisfy their information needs and provide useful guidance when it comes to protecting patron's privacy. In this paper, we conceptualize privacy in terms of the control one has (or does not have) over the disclosure of their personal information. Control has historically been a popular way of framing the concept in the social sciences and is heavily influenced by the work of Westin [2] and Altman [3], who defined privacy as "selective control of access to the self" (p. 24).

To understand how library staff are assisting patrons navigate privacy risks, we evaluated the local, state, and national policies that provide guidance to library staff on how they should assist patrons conducting online transactions, especially when it involves personally identifiable information (PII). By identifying the gaps in these

A. Sundqvist et al. (Eds.): iConference 2020, LNCS 12051, pp. 1–8, 2020.
https://doi.org/10.1007/978-3-030-43687-2_47

policies for staff/patron interactions, we make policy recommendations to ensure library staff provide the needed services without running into liability risks [4]. We also analyze data collected by our team through focus groups and participatory design sessions with library staff to get their insights on the privacy issues patrons face when using public computers, the existing procedures that work (or don't work) as staff assist these patrons; and the policies they'd like to guide patron interactions. Our research is guided by two primary research questions:

RQ1: What privacy issues do patrons face when they use public library computers?
RQ2: How do library staff navigate tensions between professional core values and patron privacy?

Based on our analysis of these data sources, we conclude this paper by presenting considerations for the development of a patron-focused privacy policy framework for public libraries. The resulting framework will provide guidelines for front-line library staff who respond to time-sensitive requests for assistance from patrons that may deal with patrons' PII.

2 Related Work

2.1 Privacy Policies in Public Libraries

A major resource for library administrators creating or revising their library's privacy policy is the American Library Association's (ALA) Privacy Toolkit [5]. This toolkit outlines how to build a privacy policy, including how to conduct a privacy audit[1] at a library and how to implement the policy once it has been created or updated. In addition to the toolkit, ALA's privacy materials include guidelines and checklists on privacy concerns like third party vendors, public access computers, and library websites [6, 7].

ALA's privacy resources provide detailed guidance on the precautions libraries as an institution should take to protect patrons' data. Similarly, much of the research on privacy in libraries focuses on library administration. For example, Pekala [8] considers privacy issues arising when third parties collect patron information, while Houghton [9] considers how to provide patrons the services they expect and still protect their privacy. Klinefelter [10] argues that circulation, reference, and interlibrary loan services are additional weak points of privacy within libraries. Building on prior work, this paper examines how libraries and library staff can assist patrons with privacy issues they face when using public computers.

[1] A privacy audit is often the first step in creating or revising a privacy policy. It evaluates current policies and practices in the library and can reveal strengths and weaknesses of existing policies and library culture.

2.2 Core Values of Librarianship

As a profession, librarians are led by a set of 12 core values that form their foundation of practice [11]. Most relevant to this paper are the values of Access, Intellectual Freedom, Service, and Privacy/Confidentiality. Access means that all information resources are equally available to all patrons. Intellectual Freedom refers to the profession's commitment "to resist all efforts of censoring library resources" [11]. Service reflects the commitment of library staff to provide the "highest level of service to all library users" [11]. While Privacy/Confidentiality states that "protecting user privacy and confidentiality is necessary for intellectual freedom and fundamental to the ethics and practice of librarianship" [11].

3 Methods

3.1 Virtual and In-person Focus Groups with Library Staff

Throughout 2017, we conducted 11 focus groups with 36 library staff at local and national library conferences and via Webex video conferences. Staff were recruited through ALA's communication channels and social media posts. Each focus group lasted approximately 90 min. Sessions included discussions on the challenges staff faced as they work with patrons, how they handle information requests involving sensitive information, and the types of resources and training they wanted to enhance their and their library's ability to resolve patrons' information needs. For a detailed discussion of data collection and analysis, see [4].

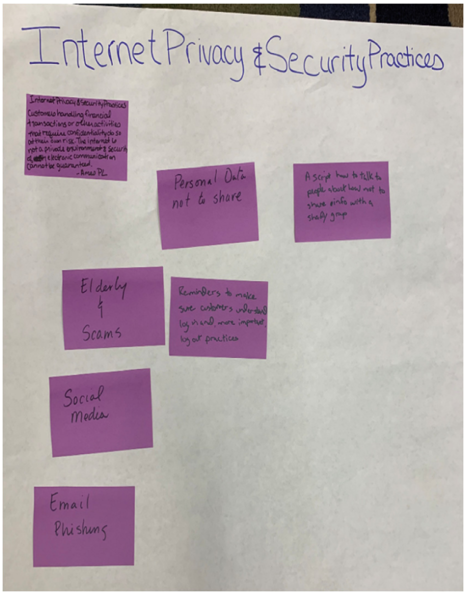
3.2 Evaluation of Local, State, and ALA Policy Guidelines

To better understand privacy issues being discussed in libraries, we conducted a review of existing policies from ALA, state libraries, and various library systems around the US. State and library system policies included in this review were gathered using snowball sampling from the ALA toolkit [5], as well as reviewing major metropolitan library systems. These policies were gathered and analyzed to develop thematic categories of privacy policies in libraries. Policies were collected until saturation was reached. In total, 16 state and public library policies were reviewed.

From these policies, we developed an initial list of eight categories for library privacy policies, including: Unlawful Use of Library Computers, Privacy at Public Terminals, Confidentiality of Patron's Search Data, Filtering, Internet Privacy and Security Practices, Rules Governing the Use of Library Computers, Guidelines for Minors, and What Staff Can and Cannot Do. These categories were then used in the participatory design sessions described below to get feedback from library staff who had experience interacting with patrons to determine what did and did not work, and what was missing in these policies.

3.3 Participatory Design Sessions with Library Staff

In the first half of 2019, we conducted four in-person participatory design (PD) sessions (see Bonsignore et al. [12] for details on PD techniques) with 24 public library staff. Two sessions were held at an ALA conference, one at a state library association conference, and one at a public library. Staff were recruited through ALA and state library channels, as well as social media. Each session lasted 90–120 min. In the first part of each session, library staff were given copies of different types of library policies (described in Sect. 3.2 above). After a large group discussion, staff were divided into smaller groups, each focusing on a different category of privacy policies. Members in each group collectively created draft policies or topics of interest that were missing in their category and added them to sticky notes. Afterward, they regrouped and discussed why these policies are needed and how these policies may vary based on communities that they serve. See Fig. 1 for an example of this process.


Internet Privacy & Security Practices
Personal Data not to share
Elderly & Scams
Social Media
Email Phishing

Internet Privacy & Security Practices Customers handling financial transactions or other activities that require confidentiality do so at their own risk. The internet is not a private environment & security of electronic communication cannot be guaranteed. -Ames PL

A script how to talk to people about how not to share info with a shady grp

Reminders to make sure customers understand log in and, more important, log out practices

Fig. 1. An example of policy ideas generated during PD sessions.

Research team members took detailed notes during each session. PD activities were audio recorded and pictures were taken. The research team transcribed the audio and created a summary document for each session that weaved the audio, observation notes, pictures, and the resulting ideas that came out of each session.

4 Findings

4.1 Privacy Issues Faced by Patrons When Using Public Library Computers

Through our focus groups and PD sessions, it became clear that library staff want to help patrons protect their data, but the rapid change in technology and new data threats make it difficult. Below, we identify three contexts emerging from our data where a patron's privacy was at risk.

Privacy Knowledge and Skills: Everyday Basics. Many patrons do not fully understand privacy risks or care about their privacy, which adds to the challenge library staff face when helping those on public computers. For example, a librarian from urban New York said, *"...many customers are not savvy at all. One man, I was questioning him about his information, and he said, 'Oh, don't worry, I'm not worth anything.' He was joking, but at the same time, that's their attitude. It's like, 'What's to steal?*'" In addition, library staff said many patrons are unaware of the digital traces they leave behind when using public computers, like not logging out of an account or storing credit card information on a retail site. Another New York-based librarian noted, "*They know there are certain things that need to be kept secure, but when they're done with their session, they're done, and they don't think about closing things out."* This issue is exacerbated for libraries that don't have safety protocols in place to delete personal information after each use. From our conversations with library staff, policies and technology for clearing user history varied significantly across library systems.

Library staff spend a lot of time helping patrons with passwords. A tech services coordinator in rural Tennessee, estimated they help patrons reset a password at least three or four times a week. Some patrons expect staff to remember their passwords for them; a librarian from suburban New York said, *"I've definitely had...patrons who are like, 'Why can't you remember it?' And it's like, we see hundreds of you guys every week. We can't remember all of your email addresses…We don't want to know your passwords."*

Privacy While Obtaining Critical Government Assistance. As described in Thompson et al. [13]—and as shared by library staff we spoke with—government and social service agencies often send patrons to libraries to get help with online assistance programs. These forms require transmission of PII, which makes it challenging to assist patrons in completing the forms. A librarian from urban New York noted, *"I've had folks come in and say, 'Oh, I'm just going to give you all my tax information. I need you to fill this out for me.' I can't sit down and do that for them as a librarian… I can help point you in the right direction, but I'm not allowed to put in any information for you."*

Privacy When Accessing Library-Contracted Third-Party Vendor Sites. An emerging concern that library staff have is the amount PII collected by third-party vendors who have contracts with library systems. Oftentimes, patrons have no idea when they move from a library site to a third-party site while using the public computers. Like Houghton [9], several library staff expressed concerns regarding the amount of data third parties collect and how to inform patrons regarding third-party data sharing policies. A branch manager from urban North Carolina expressed their concern over third parties, saying, *"[I was] talking to [a] vendor about novels and whatnot...and he was like, 'Have you heard about linked service, using GPS to see how* *close you are to the library…' Makes me nervous…to see what's close by and whether a book is on the shelf."*

4.2 Staff Tensions Between Their Core Values and a Patron's Privacy

Below, we discuss how library staff navigate the tensions between some of their professional values (like Intellectual Freedom, Access, and Service) and the core value of Privacy and Confidentiality.

Providing Access to Information vs. Preventing Risky Privacy Practices. Staff we spoke to had an expectation of neutrality when it came to digital privacy and security, in line with core values of Intellectual Freedom and Access. They discussed challenges they faced when trying to balance helping their patrons and preventing them from making risky decisions. As a librarian from Washington D.C. noted, the goal is to *"communicate the risks without dictating what they can and cannot do."* Similarly, another librarian from Maryland described the expectation that library staff remain neutral: *"I think that's what can get tricky helping serve customers because sometimes they're doing something that probably isn't the best privacy practice…and trying to remain that neutral party or give them verified resources to assist them."*

In practice, however, risk assessment by library staff seems largely idiosyncratic, rather than based on specific policies. Other library staff we spoke with described situations where they explicitly warned patrons about risky situations. A tech services coordinator from rural Tennessee said, "*If [you] see something on there that they really shouldn't have on [their] device, you're like, 'Hey, this is spyware, you need to get rid of this.' …You cross a very fine line of wanting to help your patrons while trying to stay neutral."*

Library staff also recognize that libraries are trusted institutions [14] and that this trust goes hand in hand with neutrality. A librarian from urban California explained, *"I think a lot of it, is patrons trust the library. We're the neutral place where it's okay. No one's going to come after them. Whatever they share stays with us… So they're always willing to share information. And sometimes, I feel like they share a little bit too much."*

Providing the Highest Level of Service vs. Protecting Patron's Privacy. Many library staff we spoke to struggled to find a balance between providing high-quality service to patrons while still protecting their privacy. A librarian from urban California explained, *"I think a lot of patrons are so desperate to get assistance…[that] I don't think they realize they are handing us sensitive or private information."* A librarian from urban North Carolina had similar experiences: *"We get people who are in a hurry and just wanna get something done really, really fast. So they'll want us to do things that are beyond that policy. And that's when we have to say, 'This is your task and we will show you how to do it, but you need to do it yourself.'"*

Some patrons prefer library staff complete their computer tasks because of physical disabilities or a lack of digital literacy. This creates an additional strain on library staff between following stated policies and recognizing many situations fall into gray spaces. A librarian from urban Maryland explained how they handle these situations: *"…if it becomes overwhelming, like, 'okay, I really need you to bring someone with you to help* *you,' that's some of the ways that I've dealt with working with customers and their sensitive information."*

5 Discussion

This analysis is part of a larger research project, with a goal of developing a patron-focused privacy framework to guide US library staff in assisting patrons with their information needs and encourage patrons to develop privacy skills and keep their information secure in public spaces. The themes presented in this paper form the basis of this patron-focused framework that will be created to be used as a companion to the existing ALA privacy toolkit [5]. ALA's privacy framework focuses on how libraries can protect patron's data but does not fully address how library staff can help patrons protect their own information on public computers.

We asked library staff to talk about the utility of policies or other resources they could use when helping patrons navigate privacy risks and the tensions described above. The overwhelming response was that while it was an appealing idea, the process of building a privacy policy focused on staff/patron interactions is easier said than done. As staff responses have highlighted, patrons' privacy skills, interest, and knowledge vary significantly, and their expectation and trust with library staff assumes that staff are comfortable handling their PII. This variation creates challenges for designing a framework that can be applied to many different library contexts.

To make this framework applicable to all libraries and library staff, the completed framework should be flexible enough to allow for variations in situations/contexts while still providing enough guidance for library staff on where to draw the line. To be inclusive and scalable, the framework should be written in a straightforward language—not full of technical jargon. In addition, any privacy framework needs to be general enough to allow for changing technology and any new privacy risks that will arise.

When discussing what types of content are most important for a policy resource, most staff stressed that discussions of privacy should be connected to patrons' everyday technology use rather than covering high-level topics like encryption. The framework should also address the three contexts we discussed above – basic privacy knowledge, privacy when completing government forms, and privacy when using third party sites. Additionally, the framework should address the tensions between librarians' core values and privacy concerns by providing suggested solutions that work best for their own library system and population.

6 Conclusion

This study provides an important step in developing a privacy framework that allows library staff and administrators to personalize policy based on their branches' privacy configurations and patron population. Next, we will be co-creating this patron privacy framework through PD sessions with library staff and sharing examples with the larger library community across the US. We will work with technology policy and privacy scholars to ensure policy language alleviates the tensions library staff have indicated in this study, as well as allowing patrons to safely utilize public computers in the libraries to complete everyday transactions.

References

1. Mobile Technology and Home Broadband 2019. https://www.pewinternet.org/2019/06/13/mobile-technology-and-home-broadband-2019/. Accessed 16 Sept 2019
2. Altman, I.: The Environment and Social Behavior: Privacy Personal Space Territory and Crowding. Brooks/Cole Publishing Co., Monterey (1975)
3. Westin, A.F.: Privacy and Freedom. Atheneum, New York (1967)
4. Vitak, J., Liao, Y., Kumar, P., Subramaniam, M.: Librarians as information intermediaries: navigating tensions between being helpful and being liable. In: Chowdhury, G., McLeod, J., Gillet, V., Willett, P. (eds.) iConference 2018. LNCS, vol. 10766, pp. 693–702. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-78105-1_80
5. Privacy Tool Kit. http://www.ala.org/advocacy/privacy/toolkit. Accessed 15 Sept 2019
6. Library Privacy Guidelines. http://www.ala.org/advocacy/privacy/guidelines. Accessed 07 Sept 2019
7. Library Privacy Checklists. http://www.ala.org/advocacy/privacy/checklists. Accessed 07 Sept 2019
8. Pekala, S.: Privacy and user experience in 21st century library discovery. Inf. Technol. Libr. **36**(2), 48–58 (2017). https://doi.org/10.6017/ital.v36i2.9817
9. Houghton, S.: The challenge of balancing customer service with privacy. J. Intell. Freedom Privacy **4**(1), 8–9 (2019)
10. Klinefelter, A.: Privacy and library public services: or, I know what you read last summer. Legal Ref. Serv. Q. **26**(1–2), 253–279 (2007). https://doi.org/10.1300/J113v26n01_13
11. Core Values of Librarianship. http://www.ala.org/advocacy/intfreedom/corevalues. Accessed 07 Sept 2019
12. Bonsignore, E., et al.: Embedding participatory design into designs for learning: an untapped interdisciplinary resource. In: CSCL 2013 (2013)
13. Thompson, K.M., Jaeger, P.T., Taylor, N.G., Subramaniam, M., Bertot, J.C.: Digital Literacy and Digital Inclusion: Information Policy and the Public Library. Rowman & Littlefield, Lanham (2014)
14. Gomez, R., Gould, E.: The "cool factor" of public access to ICT: Users' perceptions of trust in libraries, telecentres and cybercafés in developing countries. Inf. Technol. People **23**, 247–264 (2010)