Libraries' Approaches to the Security of Public Computers

Samuel Dooley, Michael Rosenberg, Elliott Sloate, Sungbok Shin, Michelle Mazurek
University of Maryland – College Park
{*sdooley1, micro, esloate, sbshin90, mmazurek*}*@umd.edu*

Abstract

Beyond providing books to the general public, one of the primary roles of the public library in the modern age is to provide computer and internet access to its patrons. Those without a smartphone or personal computer often rely on public-access computers, wifi, and printers to perform necessary tasks such as reading email, banking online, researching topics of interest, and communicating with loved ones. This makes clear the need to protect and preserve the privacy and security of the patrons who use these public devices. Unfortunately, there has been little research on the security measures taken by public libraries. In this paper, we present a pilot study on the measures public libraries take in order to ensure patron privacy when using these devices. We use semi-structured interviews to elicit information about security practices, policies, and constraints. We analyze the results and give tentative suggestions for libraries interested in improving patron privacy.

1 Introduction

In most libraries, electronic devices, such as mobile tablets and desktop computers, are installed to aid patrons in discovering new information. These devices help patrons understand new concepts, produce novel ideas, and communicate with people around the world.

To the knowledge of the authors at the time of writing, there is no current research on the different ways in which libraries conceptualize and implement the protection of patron privacy and security specifically relating to the use of public devices. To this end, we aim to understand the kinds of problems that libraries can face in security and privacy matters. We pose two research questions which motivate our work:

RQ1: How do libraries ensure patron privacy and security on public-facing devices?

RQ2: How do libraries develop policies for the administration of public-facing devices?

To do so, we conducted three semi-structured interviews with IT or IT-adjacent professionals from 2 distinct US public libraries. We inquired about the libraries' policies, current practices, and the issues they face. We provide an analysis of some of the differences and commonalities of the libraries. Further, we offer suggestions that are intended to maximize benefit to personal privacy and security while minimizing encroachment on the constraints laid forth by the libraries.

We acknowledge that our results do not represent a significant number of libraries. But based on our work, we aim instead to explain and anticipate limitations and challenges that can possibly occur in other libraries. The issues in privacy and security we discuss are: physical security of computers, the policy-making process of privacy and security matters, privacy from malicious actors, configuration security, and session privacy.

The remainder of this paper as structured as follows: We first study the related work on libraries and technology. Then, we present the methods used for the interviews and the results of those interviews. Finally, we discuss limitations and issues regarding security and privacy in libraries.

2 Related Work

Privacy and confidentiality have been important aspects of library policy for some decades now [4, 10]. Given that recordkeeping is one of the core functions of a library, the American Library Association's (ALA) Code of Ethics saw it fit to address concerns about privacy as early as the 1960s [10]. The specific actions libraries take in protecting patron privacy and confidentiality have been shaped by laws at the national, state, and municipal level, as well as by guidelines formed by associations such as the ALA [4, 10, 1]. States have passed laws that specifically protect the confidentiality of library records, while others have modified open-record laws to address library confidentiality [10]. These state laws vary greatly in the kinds of records they seek to protect [1], which underscores the importance of national guidelines that enable libraries to craft security policies.

The ALA has published guidelines under their Library Privacy Guidelines for Public Access Computers and Networks and Privacy Tool Kit [4, 1]. The guidelines are shaped by the "Fair Information Practice Principles": Notice, Choice, Access, Security, and Enforcement [1]. These guidelines provide advice on how to enforce privacy and confidentiality in recordkeeping and computer access. The guidelines recommend that li-

braries only keep records as long as needed, and further recommend that libraries anonymize them whenever possible [4, 3]. For example, the ALA suggests that libraries regularly purge personally-identifiable information (PII) on "library resource use, material circulation history, security/surveillance tapes, and both paper and electronic use logs" [1]. In regards to computer access, the ALA recommends clearing browser and cache history after each session, and regularly checking for devices such as keyloggers that may be placed on computers to steal private information [4].

As computers became more ubiquitous, the first thing in libraries that became computerized were library catalogs. With the digitization, much work was done on the protection of patron records in these new digital formats [6, 11]. The American Library Association lays outs its principles in the ALA's Library Bill of Rights [3] and Code of Ethics [2] around libraries and privacy and equal access to information.

Beyond just library catalogs, the format of ubiquitous information changed during the computer age, as well [12]. Computers became the fastest way of looking up information, and personal computer usage became more common. For populations in which it is not common to own a personal computer, libraries became a nexus from which they can access the internet — a disparity often drawn along socioeconomic and cultural lines [5]. Important work has been done to study the impacts on these communities and identify strategies aimed to address the disparities [9, 15, 13]. Over time, some services have transitioned to only being able to be accessed via computer, particularly government services that benefit populations who often do not have home internet access [8]. This shift has changed the role of the library and librarians significantly [14].

3 Methods

Our study consists of semi-structured interviews with information technology (IT) or IT-adjacent professionals at public libraries in the United States. The study was approved by our university's IRB. Below, we describe how we developed our interview protocol, how we conducted our interviews, and how they were analyzed.

3.1 Protocol Development

Public library computers present a wide variety of security risks, particularly to the many members of vulnerable populations who rely on these computers as their only means of accessing the internet. To answer RQ1, we consulted with experts in Library Information Sciences at the University of Maryland and, together, enumerated possible threats to public computers, with special emphasis on how public computers are typically used in libraries. From this list, we identified three main areas where security or privacy could be targeted. These are listed below:

Privacy from Malicious Actors This is the privacy that a patron at a public computer has in the presence of a malicious party which has targeted that specific computer (or set of computers, or routing device) for information retrieval. Concretely, a malicious actor could use a keylogger or malware, or simply shoulder surf in order to retrieve sensitive information belonging to patrons who have used or will use the same computer(s).

Configuration Security This is the security of the computing environment that the patron uses. Potential threats to configuration security include malware, old and vulnerable versions of popular software, and non-TLS-secured web browser home pages.

Session Privacy This is the confidentiality of patron-specific session data. Threats to session privacy include sharing browser history, downloads, and application-specific data across patron sessions.

In support of RQ2, we also endeavored to understand how libraries develop policies around their public computers. We included a section at the beginning of the protocol that is intended to help us understand whether the participant's library has any policies about the administration of their public computers. If they did have policies, we asked them how the policies were developed and if they (the participant) was involved in the development process. The interview protocol can be found in Appendix A.

3.2 Interview Procedures

We recruited our participants from regional and university public libraries in the United States. Due to the nature of our research questions, we were primarily interested in speaking with the IT professionals at each library system. We did our best to identify potential participants from publicly available information on the library websites or other government resources. If this was not possible for a given library system, then we recruited from the general "Contact Us" link for that library. We aimed to produce a sample which would represent different library sizes, target populations, resources, and needs.

For this pilot study, we recruited three participants ($n = 3$) for two different library systems. We have two participants from Library A (L-A), a library with 8 branches associated with a large public university in the United States; and one participant from Library B (L-B), a public library system from a rural county in the United States with five branches.

After a potential participant responded to our solicitation, they were directed to fill out the consent form and schedule a time for the interview. Interviews were conducted over Zoom. With the participant's consent, we recorded the interview audio. At the completion of the interview, we offered the participant $20, to be received either as a gift card issued to them, or to be donated. We offered the donation option because we hypothesized that some intuitions would prohibit gifts or some participants might feel uncomfortable receiving the gift. Of the three participants, two declined both the gift and the donation, and one opted for the donation.

3.3 Qualitative Analysis

After the interviews were completed, we used the recordings for analysis. We transcribed the recordings by hand. With additional time and/or resources, we may use a transcription service in the future. Since none of us had deep prior knowledge of the field of library security, we

inductively coded our data. Due to our small sample size, we decided it would be best to consider all of our interviews when developing our codes, so we did not engage in any independent coding. We hope that the codes we have developed will be useful in future research. Additionally, the coding and analysis was done by hand in text-editing software. With additional resources and interviews to code, we might use coding software in the future.

4 Results

In this section, we outline the four broad categories described in Section 3.1. We notate our **codes** in bold, and their possible *values* in italics.

4.1 Policy Formulation

In each of our interviews, we found that libraries had multiple sources that influenced the creation of their policies towards patron security and privacy. We found that there were three main **sources of policy**: *internal sources*, *IT Departments*, and *laws/regulations*. Each library had some mixture of these sources guiding policy creation. For instance, L-B had an internal committee that played a large role in the creation and review of policies, which then were vetted by a legal department. Other, more technical aspects of their policy were delegated to IT staff. L-A relied on a large IT department for many of their computer security policies, such as login credentials and software patches, while also following guidelines for public libraries and formulating their own policies for computer usage.

We also found that there are constraints on the amount of privacy a library can feasibly provide. We grouped these sources of **constraints on security policy** into *patron needs*, *compliance with legal obligations*, and *limited budget resources*. Because libraries first and foremost serve their patrons, they may have to forego security measures to serve them in other ways. We found that L-A could not place physical dividers in between computers, as it would hinder collaboration between patrons. L-A also chose not to have a firewall, since some users had to access what a firewall would consider explicit content for their classes. Libraries may also have to cater to a high volume of patrons, which makes some physical security tasks more difficult. L-B also had been asked to provide information to federal agencies, which, of course, obligates them to collect and store some information about patrons. All the libraries we interviewed had budget constraints, which naturally has wide impacts. Budgetary constraints determined things from the physical layout of the terminals to the amount of 3rd party security software that could be purchased.

In our interviews, we saw that some security policies were very explicit and readily available for review, while others were more of an "understanding" between librarians and IT staff. Because of this, we say that libraries' **policy formality** can be categorized as *formal* and *informal* policies. We found that both libraries have a bit of both. L-A had a set schedule for pushing software updates for their all of their computers, but also conducted physical sweeps looking for "funny" things that may compromise computer security. L-B had a policy for sign-in sheets but also did not have a formal OS update schedule.

4.2 Privacy From Malicious Actors

We asked libraries about the steps they took to ensure patron privacy in the presence of an actor who may be targeting a set of terminals at the library through a number of different attack vectors.

We first examined some of the ways libraries can deter malicious actors through physical means. We asked libraries if they employ **physical sweeps**, which can be used to detect devices such as keyloggers. We categorized their response as either *frequent* or *infrequent*. L-A conducted physical sweeps multiple times a week (considered frequent), while L-B did not conduct physical sweeps at all (but expressed their desire to start them).

We also asked about the **physical layout** of the library, which can determine how safe patrons are from attacks such as shoulder surfing. From our responses, we categorized the layout as *security-focused*, *patron-focused*, or *unfocused* (meaning there was no clear intent in the layout). None of the libraries we talked to had a *security-focused* layout (though we anticipate some may in the future). L-A was patron-focused, designing their layout to maximize ease-of-use for patrons and to foster collaboration, while L-B was unfocused, as they did not have a dedicated area for computer use, and instead placed computers just where they could fit them.

We also looked at how libraries can defend against other attacks that patrons may face when using public computers. We found that each library had some form of **antivirus** installed, which is important for patron safety. However, while one of our libraries had a *secure* **wifi** system, another had an *unsecured* wifi system that was also accessible from the library's parking lot. This may leave library users' privacy vulnerable to traffic logging.

4.3 Configuration Security

To broaden the kinds of threats we anticipate library patrons may be exposed to, we looked at the configuration of software installed on the public computers. Misconfiguring or failing to correctly configure a public-use computer can leave the computer and its user significantly more vulnerable to attacks such as traffic sniffing, phishing, and general malware which does not require attackers to be in the physical vicinity of the library.

The first question we asked was about **operating system security**. In particular, we wanted to know whether a recent version of the library's preferred operating system was installed. We coded this as *up-to-date*, and *out-of-date*. L-A said they were running a recent version of Windows 10, while L-B said they were in the process of switching over from Windows 7—a version which, as of January 2020, no longer receives free security patches. Though we did not explicitly ask, we do not find it likely, given budget constraints, that L-B had opted into Microsoft's extended support program for enterprise users, which has a pay-per-device model [7].

In a similar vein, we asked about **software update frequency** and about the existence of a **critical update fast track**. L-A indicated that they do *frequent updates*, and *have a fast track* for security updates. L-B indicated that they weren't certain, though they believed that they also do both of these practices.

To make sure that users cannot intentionally or unintentionally misconfigure the computers, we asked about **user capabilities**. Broadly, we wanted to know whether patrons have *full permissions* or operate in a *restricted* setting. We found that both libraries had restricted permissions on their patron accounts.

Finally, we asked libraries what they do for **hardening software** installed on their machines. "Software hardening" refers to the configuration of software in order to decrease its remote attack surface. We coded this with *addons* and *custom configs*, where *addons* refers to browser addons which serve to improve patron privacy or security, and *custom configs* refers to the setting of software preferences. We found that L-A did neither of these hardening behaviors, while L-B used addons but did not deploy custom configs.

4.4 Session Privacy

This category encompasses security measures that can be taken to preserve the privacy of patrons' session data, i.e., browsing history, downloads, and personal documents.

The first step to securing patron session data is giving every patron a distinct login. We asked whether **login credentials** were *required* or *not required*. L-A required login credentials, while L-B did not.

Following from this, we considered **computer data storage**. We asked how patron session data was treated after the patron stopped using the computer. The coded responses were *stored data is kept behind a login*, *stored data is not kept behind a login*, and *no data is stored*. L-A stores the data (for some fixed period of time) on the computer, behind a login. Since L-B does not have user credentials, all data remains accessible on the computer without login until it is deleted by some means.

Hard drive protection (e.g., services like DeepFreeze, Windows SteadyState, and fsprotect) can benefit configuration security and session privacy — it is a good secondary way to ensure that patron session data does not survive a reboot. Both libraries *use hard drive protection*.

We asked if the library does any **PII collection** when patrons use the machines. As mentioned in section 4.1, L-A said that they *do collect PII* upon patron login in order to follow up if they "detect any malintent" after the fact. This data is also collected in order to comply with information requests issued by federal agencies. L-B said they *do not collect PII*. The only data L-B collects is usage statistics from paper signup sheets, only storing monthly aggregates.

Finally, we asked about **printing job control**. By default many printers allow the user to repeat a job, i.e., print whatever was most recently printed without regard for user account boundaries. This is a privacy concern. L-A has access control installed on the printers, so that its *jobs are not repeatable by others*. L-B has no such restrictions, and *allows jobs to be repeated arbitrarily*.

5 Discussion

Despite our small sample size in this pilot study, it is clear that the technical resources of libraries will vary wildly, with a large majority being forced to do more with less. We see that budgeting is a non-trivial constraint across the board, so any suggestions we make would have to have a high impact-cost ratio. This said, we do see some some possible future suggestions which may allow libraries to meaningfully improve the privacy of their patrons while keeping costs low.

Secure wifi hotspots It would suffice to set a password and post it on the wall. It is a straightforward exercise for a laptop user near an open network to see the web browsing patterns of anyone else on the network. Even when TLS encryption is employed, metadata is leaked. This metadata includes things like IP addresses and domain names of the remote servers that a user interacts with. Securing wifi is a straightforward task, costs very little, and makes it significantly harder for adversaries to sniff traffic.

Keep the OS updated OS patches are critical for maintaining the security of a system. Broadly speaking, the software that is most frequently targeted is the software that's most prevalent, and operating systems such as Windows, macOS, and Linux are extremely prevalent software. Applying updates regularly can be a time-consuming task, but most vendors take care to streamline the process as much as they can, since they know that these patches are often critical.

Use a multilayered approach to data storage This is a defense-in-depth method for data privacy. Public terminals should not leave a trace of their previous sessions. The most straightforward way to prevent this from happening is by requiring individual credentials for login. The second step is to prevent someone from making permanent changes to the computer, so as to prevent a user from subverting the first step. This is achieved by the use of hard drive protection mechanisms previously discussed. The third step is to prevent someone from loading their own software onto the computer. A BIOS (or UEFI) password and locked boot order would suffice to prevent the most obvious attacks. The combination of these mechanisms would make it difficult for anyone to gain access to the data of past or future patrons.

5.1 Limitations

This report has limitations arising from the small sample size and from the study design. This study, with only three participants, is not sufficiently developed to draw conclusions from — not even conclusions about what data the rest of the interviews will yield.

The study is designed with a specific goal in mind: to elicit libraries' approaches and conceptualizations of public device security. The purpose of the study is to discover the different approaches that libraries take, and report on what those are and how they differ. Even with more participants, we may identify trends between the different approaches, however, we would not be able to correlate any of their responses based on library metadata, i.e., size, number of computers, etc.

References

[1] AMERICAN LIBRARY ASSOCIATION. Privacy tool kit, 2014.

[2] AMERICAN LIBRARY ASSOCIATION. Ala code of ethics.

[3] AMERICAN LIBRARY ASSOCIATION. Library bill of rights.

[4] AMERICAN LIBRARY ASSOCIATION INTELLECTUAL FREEDOM COMMITTEE. Library privacy guidelines for public access computers and networks. *ALA. org. Accessed March 15* (2016), 2017.

[5] BECKER, S., CRANDALL, M. D., FISHER, K. E., KINNEY, B., LANDRY, C., AND ROCHA, A. Opportunity for all: How the american public benefits from internet access at us libraries. *Institute of Museum and Library Services* (2010).

[6] COOMBS, K. A. Protecting user privacy in the age of digital libraries. *Computers in libraries 25*, 6 (2005), 16–20.

[7] FOLEY, M. J. Microsoft is offering a 'free' windows 7 extended security update to some business users. `https://www.zdnet.com/article/microsoft-is-offering-some-enterprise-users-a-one-year-windows-7-extended-security-update-promo/`. Accessed: 2020-05-16.

[8] JAEGER, P. T., AND FLEISCHMANN, K. R. Public libraries, values, trust, and e-government. *Information technology and Libraries 26*, 4 (2007), 34–43.

[9] JOHNSON, C. A. How do public libraries create social capital? an analysis of interactions between library staff and patrons. *Library & Information Science Research 34*, 1 (2012), 52–62.

[10] NEUHAUS, P. Privacy and confidentiality in digital reference. *Reference & User Services Quarterly 43*, 1 (2003), 26–36.

[11] STURGES, P., DAVIES, E., DEARNLEY, J., ILIFFE, U., OPPENHEIM, C., AND HARDY, R. User privacy in the digital library environment: an investigation of policies and preparedness. *Library Management* (2003).

[12] THOMPSON, K. M., JAEGER, P. T., TAYLOR, N. G., SUBRAMANIAM, M., AND BERTOT, J. C. *Digital literacy and digital inclusion: Information policy and the public library*. Rowman & Littlefield, 2014.

[13] VÅRHEIM, A. Gracious space: Library programming strategies towards immigrants as tools in the creation of social capital. *Library & Information Science Research 33*, 1 (2011), 12–18.

[14] VITAK, J., LIAO, Y., KUMAR, P., AND SUBRAMANIAM, M. Librarians as information intermediaries: Navigating tensions between being helpful and being liable. In *International Conference on Information* (2018), Springer, pp. 693–702.

[15] WARREN, M. The digital vicious cycle: Links between social disadvantage and digital exclusion in rural areas. *Telecommunications Policy 31*, 6-7 (2007), 374–388.

A Survey Protocol

Introduction

Hello. My name is [INSERT NAME]. I am part of a group of graduate students at the University of Maryland — College Park working on a project to understand how public terminal security is implemented in libraries. We know that libraries have a very long history of being excellent resources of privacy for their patrons. We also know that computer privacy and security is very complicated and we hope that through this research we can help libraries understand the state of computer security research. To begin this process, we are conducting this survey to discuss your library's policies and practices relating to the protection of public computers used by library patrons. I'll call your attention back to the consent form which you previously electronically agreed to. Do you have any questions about it, before we begin? First, let's quickly go over how the study is going to work. I'll begin by asking you a little about your job and history in libraries. Then, I'll ask you some questions about how your library approaches the security of the computers in your libraries that patrons use. These questions will be broadly put into three categories: physical privacy, configuration security, and session privacy. There are many reasons for not knowing an answer or being uncomfortable with responding to a question. At any time, you may choose to indicate that you don't know or would not like to answer a question. Finally, we would like to record these interviews so we can go back to them and code your responses to be aggregated with other libraries. Is it okay if I record this interview? [If they agree, then start recording. If not, end interview] Do you have any final questions before we start? Background To begin our discussion, I'm going to ask you about your experience in information technology and libraries.

1. What is your job description at [Insert Library Name]? (Ensure they describe an IT role)

2. How long have you been doing IT?

3. How long have you been doing IT in libraries, specifically?

Now I'll ask you some questions about your specific library/system and how policies and practices are decided upon. Remember, you needn't answer if you don't know or are don't want to discuss.

1. Can you explain to me how policies are developed in your library system?

2. Does your specific library have a policy relating to the administration and oversight regarding the public computers in your library?

3. Does it have sections that pertain to the protection of user data while using them? (Can you please detail what the policies are at a high level?)

4. Does it have sections that pertain to the physical security of the computer? (Can you please detail what the policies are at a high level?)

5. Specifically, can you detail how the policies were developed for the public computers? (Were you involved in the development of these policies?)

6. If there are multiple branches in your library system, how do the policies apply to them?

Privacy from Malicious Actors

We will now transition to asking more specific questions about three areas of computer security relating to libraries: privacy from malicious actors, configuration security, and session privacy. Let us start with Privacy from Malicious Actors. This refers to the privacy that a patron at a public terminal has in the presence of a malicious party which has targeted that specific public terminal (or set of terminals, or routing device) for information retrieval. Concretely, a malicious actor could use a keylogger, shoulder surfing, or malware to retrieve information about other patrons who have used or will use the same terminal(s).

1. How does your library protect the physical privacy of its patrons at its public-use terminals?
   (a) Do you have physical dividers between terminals?
2. Where are the computers located in the library?
   (a) Are computers in a separate room/space?
   (b) Are there separate computers for children and adults? Are they treated differently?
   (c) Are computer screens visible from a librarian's desk?
   (d) Are computer screens visible to someone walking by on the street or a public facing window?
   (e) Are computer screens visible to security cameras?
3. What steps do you take to secure the library WiFi?
4. Are the terminals monitored for hardware abuse? Threats include keyloggers, network monitors, concealed USB drives, etc.. Examples over monitoring could include overhead cameras or periodic physical sweeps.
   (a) If so, how frequently do sweeps occur?
   (b) How do you do them?
5. Are the terminals monitored for software abuse? Threats include malware, and changing of system or software configuration.
   (a) If so, how frequently do sweeps occur?
   (b) How do you do them?
6. Do you set a BIOS password? Do you set a device boot order?

Configuration Security

Let's transition to asking about configuration security, which refers to the security of the computing environment that the patron uses. Potential threats to configuration security include old and vulnerable versions of popular software, allowing MS Word macros to run by default, and non-SSL-secured web browser home pages.

1. What operating systems does your library use for its public computers?
2. How do you determine which software is on your computers? What software is on your computers? What OS?
3. How do you configure the software?
   (a) Is there a set of guidelines or best practices you follow?
   (b) Do you have any documents or websites that open on application start (e.g., Firefox homepage)?
   (c) What do you do with Microsoft Office?
   (d) What do you do with Adobe Acrobat?
4. How do you update software, and how often? Note that some software versions become unsupported after some time and require a new license purchase for security updates.
   (a) Do you distinguish in your process between security updates and other updates? Is there a fast track?
5. Who in the organization is responsible for these types of actions? Is it contracted out to a third party? If so, whom?
6. How do you ensure multiple computers all get the same configuration?
7. Have you heard of session management tools like DeepFreeze or Windows SteadyState ? Do you use it? What do you think of it?

Session Privacy

Our last big section focuses on session privacy, which refers to the confidentiality of patron-specific session data. Threats to session privacy include sharing browser history, downloads, and application-specific data across patron sessions.

1. How do you manage which patrons use which terminals and when?
   (a) Are the time or frequency limits set on the use of computers?
   (b) How, if at all, do patrons reserve time on the terminals?
2. Do patrons log in and out of the terminals?
   (a) What happens upon login and logout? What, if anything, gets wiped?
   (b) What happens upon reboot?
3. 3. Does the library filter or firewall internet content on any of its computers? If so, where are the logs stored?
4. How often do print or scan jobs stay on your printing or scanning devices? Do you have access control mechanisms set up on these devices?
5. Do you rent out laptops? How do you provision laptops? What do you do once they're checked back in?

Wrap Up

That concludes the main portion of the survey.

1. Do you have anything else to tell us that you think would be useful for us to know about libraries in general or the use of public computers?
2. Based on your understanding of our research goals, do you think that we missed any large portions of security and privacy relating to the use of public computers in libraries?
3. Is there any specific piece of information you told us that you would like us not to share in our final report?

Thank you so much for your time by taking this survey. We would like to offer you $20 for your time and participation. We can provide this to you as an online gift card. Note that some institutions have rules around receiving gifts. If that applies to you, we can also make a donation in your name. Would you like the gift card or the donation?