How Library IT Staff Navigate Privacy and Security Challenges and Responsibilities

Alan F. Luo*
University of Maryland

Noel Warford*
University of Maryland

Samuel Dooley
University of Maryland

Rachel Greenstadt
New York University

Michelle L. Mazurek
University of Maryland

Nora McDonald
George Mason University

Abstract

Libraries provide critical IT services to patrons who lack access to computational and internet resources. We conducted 12 semi-structured interviews with library IT staff to learn about their privacy and security protocols and policies, the challenges they face implementing them, and how this relates to their patrons. We frame our findings using Sen's capabilities approach and find that library IT staff are primarily concerned with protecting their patrons' privacy from threats outside their walls—police, government authorities, and third parties. Despite their dedication to patron privacy, library IT staff frequently have to grapple with complex tradeoffs between providing easy, fluid, full-featured access to Internet technologies or third-party resources, protecting library infrastructure, and ensuring patron privacy.

1 Introduction

Libraries serve as a central hub for technology access for a large number of people in the U.S. and in other Western countries [25, 45]. As people require technology access for things like searching for jobs, education, and accessing essential services, libraries provide this access to many users, particularly those who cannot afford personal computing devices. This well-studied phenomenon is sometimes referred to as the "digital divide" [59]. Further—in contrast to earlier notions of the digital divide—access to infrastructure is not the only or even most important barrier: digital equity also encompasses ease and quality of use [24].

As a free and public service, which for many users is the only or primary means of technology access, the security and privacy of library IT resources can be critically important, in multiple dimensions. First, when patrons[1] are reliant on libraries for all or most of their computing needs [60], their usage includes potentially very sensitive activities. For example, LGBTQ+ people [19], teenagers [63], people who have experienced intimate partner surveillance or violence seeking out information resources that they must keep private from others in their households [37], or marginalized and older individuals filing taxes [39] may be more susceptible to threats. Second, patrons may not be as familiar with assumed-to-be "standard" self-protective behaviors that many home computer users have learned [49]. For example, Madden [35] argues that low socioeconomic adults struggle to find resources on how to protect their online data, and are uniquely vulnerable to privacy risk, perhaps due to increased dependence on mobile internet technologies in the absence of home broadband connectivity. This increases the importance of security and privacy protocols adopted by librarians. Third, and relatedly, the types of risks that vulnerable and marginalized patrons perceive might be different from (or put them at odds with) what is commonly expected when we think of privacy literacy [36, 38, 62].

Library IT staff members can make security and privacy decisions that have a direct impact on these marginalized individuals, who may turn to the library for privacy information [34], or for essential computing resources [26, 46] that put them potentially at a higher risk for privacy violations [35].

This paper reports on interviews with 12 library staff members from the U.S who are responsible for technology management at their libraries. The participants span a variety of roles—from one of many on a large IT team, to library director who doubles as system administrator—at a variety of institutions—from small rural libraries to large library systems in major cities.

Research Question and Contributions We approached this research with the broad research question:

> What kind of privacy tools and strategies (if any) do library IT staff provide for their patrons, and why?

We frame our findings using Sen's capabilities approach [54], which allows us to go beyond specious notions of access and usage to illuminate the tradeoffs that library IT staff consider when they make decisions about privacy in

*These authors contributed equally to this work.

[1] A "library patron" (hereafter, "patron") is someone who uses a library service.

the service of patron freedoms. We will show that library IT staff provide critical resources for supporting Sen's notion of expansion of freedom, particularly in the sense of making information available [54].

We find that library IT staff are more concerned with protecting patrons from external threats (e.g., governments and institutions that sell their data to third-parties, which they believe infringe on patron freedoms [54]) than with protecting library systems from potentially malicious patrons. For this reason, librarians are most concerned with ensuring that patron data is not stored, even if it requires that they exert less oversight. At times, library IT staff must make difficult tradeoffs in enabling patron capabilities—for example, between supporting patrons in achieving their IT goals (availability and maximum utility of services) and protecting privacy (confidentiality). As might be expected, library IT staff struggle with lack of resources and training, as well as conflicts with decision makers and other organizations, resorting in some cases to creative or unorthodox solutions in order to uphold these patron freedoms.

2 Background and related work

Libraries in the U.S. [3] and in other Western countries [6] are staunch guardians of their patrons' right to free access to information, which has historically required protection from governments and other entities.

Librarians' role as guardians of patrons' privacy and intellectual freedom has, at times, been in tension with their civic role to defend public safety and security [12, 58]. The challenges librarians face today are even more complex, spanning government institutions as well as the third-party entities that provide digital resources to patrons, not to mention the vast space of digital resources and media that originate beyond library walls, but which are accessed using library computers.

In the last decade, librarians have had to contend with privacy incursions from the Department of Homeland Security (DHS), who sought to bar libraries' use of privacy technology like Tor [5], and the FBI, who used the National Security Letter (NSL) provision of the Patriot Act to subpoena patrons' records. At each point, librarians fought back through legal means, but also directly at their libraries. Perhaps the most well known example is related to NSLs, when some libraries posted signs saying that the FBI had not been there but to watch closely for the removal of the sign to indicate that the FBI had requested patron records [21].

More recently, library scholars have focused on the way in which surveillance capitalism and big data policing [9, 17, 30, 66] implicates libraries that rely on third-party products. These products amass patrons' personal data, which may then be sold to law enforcement entities, including Immigration and Customs Enforcement (ICE) [30]. Consolidation of the major publishers has left librarians little choice but to be dependent on these vendors.

This creates a dilemma for libraries who want to both provide free access and protect their patrons' privacy. According to Lamdan [30], libraries may indeed see their role as being on the front lines, acting on behalf of their patrons, where policy has failed. Yet, this complex set of adversaries introduces new challenges and tensions in librarians' role as guardians of patrons' privacy.

The American Library Association (ALA) has recently weighed in on these types of dilemmas [4]. The ALA has staunchly opposed efforts by top academic publishers like Elsevier, Springer, and Nature to clamp down on illegal use of academic material through the use of surveillance software, including collection of biometric data [40]. According to a 2021 resolution, the ALA "stands firmly against behavioral data surveillance," citing the "Intellectual Freedom Manual" [18] to ensure that librarians protect patrons from misuse of their data, including by the library itself [4]. The resolution also calls on librarians to uphold their role as advocates for their patrons' privacy and confidentiality, and to continue to educate themselves to ensure they can fulfill this role. Libraries aim to hold themselves to privacy standards defined in the Library Code of Ethics, first published in 1939 [2]; when vendors do not meet those standards [29], it is not entirely clear how they reconcile this tension.

In addition to threats from governments and vendors encroaching on protecting patron privacy, libraries must also consider privacy concerns relating to state and national law (e.g., the California Consumer Privacy Act, or CCPA) [15], as well as patrons' privacy on social media [31]. Further, many patrons rely on libraries' digital resources to, for example, seek health information or look for jobs [25], making libraries a space where sensitive data is transmitted on public computers. A survey conducted by the Pew Research Center in 2016 found that 29% of patrons 16 years or older used library computers [26]. Among those patrons, 61% use them for research for school or work, 38% use them to get health information from online resources, and 26% use them to take online classes or complete online certifications. An older report from 2012 breaks down patron PC usage slightly differently, reporting that some 41% of patrons used public PCs to visit government websites or get information regarding government services, and 36% of patrons used them to look or apply for jobs. While these numbers may have changed in the intervening time, it is likely many patrons still use library resources this way [65].

While the literature points to efforts being made to study and inform librarians' privacy practices, (e.g., [33]) there has been little systematic research focused on how librarians perform privacy stewardship, what their priorities are, and what technologies they use to reflect their priorities. In particular, there has been little study of those serving the role of library IT staff. Here, we begin to address this gap.

2.1 Low-income marginalized communities and library privacy

Low-income marginalized[2] individuals face a "matrix of vulnerabilities" stemming from primary dependence on mobile technologies for internet access, further hampered by lack of use or familiarity with internet privacy tools and strategies [35]. Not only are low-socioeconomic individuals more reliant on public computers [26], they may lack strategies for keeping their information safe online [34].

Vitak et al. show how librarians struggle with providing assistance to patrons who rely on library computers for sensitive transactions, especially when these patrons lack concern or tools for protecting their data and/or trust librarians implicitly with their personal data (which extends to online sites) [60]. Yet, research has also shown that libraries may lack formal privacy strategies for protecting their patrons' privacy, leaving librarians to take an ad hoc and often intersectional approach to protecting their patrons [39].

In their study of security and privacy practices of refugees in the United States, Simko et al. find that refugees, having little or no experience with certain online threats, are at higher risk for scams. Moreover, the authors find that refugees tend to rely on public libraries, community centers, and NGOs, as well as teachers and case managers, for support with sensitive data required by employers, but that this trust can be complex [56]. Further, marginalized individuals in the U.S. often experience a broader set of privacy incursions stemming from their encounters with institutions of the government. Low income, black communities are more often subject to policing and surveillance in their neighborhoods [10, 17, 32].

Immigrants in the U.S. also have to contend with pervasive surveillance. Kalhan points out that immigration governance in the U.S. has rapidly (and invisibly) been transformed into a surveillance "technology-driven enterprise" [27], with U.S. Immigration and Customs Enforcement (ICE) operating a kind of "dragnet," and that fear of surveillance is a deterrent for "immigrants and their families from participating in a broad range of activities necessary for health and well-being not only of individuals, but of the communities of which they are part" [20]. We (echoing the library IT staff participants we interview) consider access to information and computing resources that allow one to access social services, health information, search for employment, etc. as some of these necessary activities.

2.2 The capabilities approach framing

We used Amartya Sen's capabilities approach to interpret our findings. His framework centers freedom to achieve wellbeing as a moral imperative and posits that this freedom must be understood in terms of people's capabilities. We found that it usefully described the way that library IT staff are thinking about patron access in terms of what they are able to do.

Library IT staff experienced privacy tensions when providing internet resources. However, these tensions arose not simply in providing direct access to these resources, but in more nuanced navigation of capabilities (patrons using internet resources to e.g., do work or educate themselves), which were related to the specific context of their patrons and the structural barriers they faced. This mismatch between literal measures of "digital divide" success (i.e., internet access) and the nuanced needs of library patrons finds parallels in the capabilities approach. Both Sen [53] and Martha Nussbaum [41] (who has extended the framework) offer a critique of economic discourse focused on standard of living, arguing that the focus should be on well-being of a given community.

Sen first proposed the capabilities approach [53] as a way of measuring what people are capable of doing with the means provided them. It assumes a moral paradigm in arguing for the capabilities (also called "freedoms") to achieve well-being understood in terms of people's capabilities, which when enhanced increase their capabilities.

In Sen's capabilities approach, "functionings" encompass what an individual may value "doing or being," like being healthy or having a home and safe place to live. Capabilities describe the set of functionings a person has available to them, from which they can choose. In other words, capabilities represent the freedom of an individual to choose between sets of different functionings, according to their own values, in service of a "good life" [54].

Sen enumerated specific exemplar capabilities, including economic opportunities, political freedoms, social facilities, transparency guarantees (in terms of information and relationships between people), and protective security. At the same time, Sen emphasizes that the choice of which capabilities to value must be left to individuals and communities. Individual capabilities (e.g., freedom from surveillance) may be more highly valued in particular communities because of their relevance to that community's experiences and their relationship to other capabilities.

More recently, scholarship has applied Sen's framing to ICT for development, focusing on access to information [42, 64]. Wresch considers that while the number of websites in developing countries falls far behind Western countries, perhaps the availability of "helpful" local web resources is what is most important [64]. Kleine applies Sen's concept of capabilities development to ICTs in Chile, arguing that by giving individuals greater access to information, they contribute to one concept of capabilities [28].

While Nussbaum [41] further articulated specific capabilities (e.g., "life," "bodily health," "bodily integrity", etc.), we follow Sen and allow participants to define relevant capabilities rather than relying on Nussbaum's categories. While

[2] "Marginalized" here refers to the disadvantages experienced by those who are prevented from obtaining full membership and participation in society, often because of their race, ethnicity, gender, religion, sexual orientation, and/or sexual identity [44], which can overlap with lower socio-economic status.

Nussbaum's capabilities, which have recently seen considerable use in privacy and human-computer interaction fields, are useful in elevating the importance of human dignity across cultures, Nussbaum has been criticized for defining capabilities in a Western-centric way. We agree, in this context, with Sen that capabilities are more usefully defined by those who have insight into the day-to-day experiences of their patrons (and the nuances of what constitutes good access), including library IT staff. We believe this approach is more intersectional and appropriate, given that every community has its own matrix of power that makes certain identities vulnerable in certain specific ways [14]. We use this framing in our results and in our discussion.

3 Methodology

Here, we describe our interview study and data analysis.

3.1 Recruitment

To recruit participants, we reached out to candidates directly via email using information available on public websites for libraries. We specifically emailed candidates who identified as information technology specialists for the libraries they worked at. We also posted advertisements on public fora, including Reddit and Twitter. We also reached out via email to library staff in our personal networks to ask for referrals to IT staff. As the study progressed, we also relied on snowball sampling to recruit additional participants. We asked participants if they had connections to other library IT staff that might be willing to interview with us. Participants were considered eligible if they were 18 or older, were employed at a public or university library, and their job included IT work (formally or informally). We also accepted participants currently working in a library advocacy organization who had prior IT experience in a library.

Participants who responded were asked to complete an intake survey (to provide background information to the interviewer) and then scheduled for an interview.

The study was approved by the University of Maryland IRB. Participants were asked to complete separate online consent forms prior to the intake survey and the interview. The consent form described the purpose of the study, the researchers conducting the study, the study procedure, and how interview recordings, participant names, and contact information would be handled. Participants were also asked prior to the interview if researchers could record the audio of the interview for analysis, and were informed that they could stop the interview at any point or decline to answer any questions. Participants were also explicitly informed that recordings might be sent to a third-party transcription service.

3.2 Intake survey

Participants who expressed interest in interviews were asked to complete an intake survey including questions which characterized the size and type of library they worked at, their experience with IT in libraries, summary information about the computing resources provided by their library, and vulnerable populations their library served.

Information about technology use and staffing was used to guide interview questions—for example, if the participant described working with contractors to provide IT services in the intake survey, we asked about those contractors in the interview. The intake survey also provided context for the responses for each participant.

3.3 Interview protocol

One researcher conducted the 12 semi-structured interviews via video conference. These interviews were audio-recorded and automatically transcribed, supplemented by notes taken by the researcher. The consent form explicitly noted the possibility of third-party transcription when participants were asked about audio recording. Interviews lasted, on average, about one hour, and participants were compensated with a $35 USD Amazon gift card. The intake survey and interview protocol are hosted at https://osf.io/f589r/?view_only=aec8a186e8b84f7c860d35eda7857dea. We asked participants about a wide range of topics, including:

Role and responsibilities. We asked participants about their day-to-day responsibilities at their organization. We also asked how participants ended up in their roles and what they thought about those roles.

Staffing structure. Participants were asked to describe the structure of IT staffing at their organization, as well as who they reported to, and how many employees responsible for IT operations their organization employed.

Patron populations. We asked participants to talk about the patron population that their organization served, how many patrons they served, and the ways that patrons typically used the library services. We also explicitly asked about populations that are historically underserved or face higher-than-average digital-safety risks, and how their organizations were serving those patrons.

IT services and infrastructure. Participants were asked to describe the kinds of IT services their organization offered, such as public PCs, internet access, and printing services. We also asked about how those services were offered and managed, specifically whether the organization self-managed these services or if they contracted third-party vendors to do it for them.

ID	Institution	Years in: Library IT	Total IT	# IT staff	Est. patrons/month
1	Advocate organization	2	8	2	-
2	City library system	2	2	3	48K
3	University library	2	2	-	-
4	City library branch	1	1	17	300K
5	County Library system	10	22	14	100K
6	Association library	9	9	1	-
7	Local library system	7	9	1	-
8	Advocate organization	12	12	18	408K
9	Advocate organization	20	20	-	-
10	City library system	1	2	1	22K
11	Local public library	10	10	1	3K
12	City library branch	2	2	-	50K

Table 1: Participant information including the type of institution they were affiliated with, work experience in IT (in a library setting and overall) the number of IT staff at their institution, and the estimated number of patrons their institution serves per month. Items are left blank when participants did not know or preferred not to answer.

Security and privacy policies and tools. We asked participants about the specific security and privacy policies and tools they regularly employed to protect their infrastructure and their patrons. We also asked whether they felt that those policies and tools were sufficient to meet the security and privacy needs of their organizations.

Security and privacy challenges. Participants were asked about specific security and privacy challenges that they regularly face at their organization, and whether or not they felt they were adequately addressing them at the moment. In some cases, we also asked about what participants felt would need to be done to resolve those challenges.

COVID-19 pandemic. We also asked about how the COVID-19 pandemic affected the typical operations of their organization and whether or not that impacted the security and privacy considerations of IT staff.

3.4 Participants

We recruited 12 participants in Fall and Winter of 2020. Participants worked at libraries ranging from rural to urban, with a wide range of experience and educational backgrounds. The particular positions these participants held varied—one participant was the director of a small, rural library in addition to being responsible for the IT concerns of this library, whereas multiple participants worked as part of an IT-specific team at large, metropolitan library systems in major U.S. cities as library IT staff. Three participants currently work for advocacy organizations rather than directly for a library, but all three had library IT experience—this experience, in fact, was what drove them to advocacy in the first place. Some participants had backgrounds in computer science or information technology, but many had library science backgrounds. Participant institution types, IT experience, staff size, and estimated patrons served per month are presented in Table 1.

3.5 Thematic analysis

Two researchers from the team conducted a reflexive thematic analysis (RTA) [7, 8]. After reading through all the transcripts, they generated initial codes that were applied to a sample of interviews and discussed. These researchers met with the team to further discuss these codes and potential research themes. They then continued to iterate on and apply these codes to the remaining interviews and developed a set of refined themes. Codes were first categorized, then discussed and further refined with the research team over the course of several meetings, as themes were developed. The two researchers continued to code the remainder of the transcripts. After developing the themes, we assigned illustrative quotes. We ultimately generated four high-level categories (goals, responsibilities, tensions, constraints). Within these categories, we identified our themes (formatted in bold below). We applied Sen's capabilities approach framing to interpret our findings.

To develop our themes, we engaged with Braun and Clarke's most recent perspectives on RTA [8], developing themes flexibly and organically, while comparing and testing them for coherence and consistency. The resulting themes organize salient, meaningful segments of the data.

3.6 Limitations

As is typical for qualitative studies, our goal is not to be fully generalizable, but rather to identify key themes and ideas

related to our research questions.

Our sample size of 12 is relatively small, but is well within norms for human-computer interaction studies [11] and qualitative best practices [23]. To broaden our results, we recruited from many types of libraries in a wide variety of U.S. locations; however we acknowledge that other IT staff working in public libraries, especially in other countries, may have different experiences. Nonetheless, we believe that the themes we discuss here are highly relevant to the greater library IT space, even if they are not generalizable to all libraries.

Additionally, the researcher who conducted the interviews was different from the researchers who performed the thematic analysis on the interview transcripts. The researchers who performed the thematic analysis discussed the interviews with the interviewer and were careful to immerse themselves within the data sufficiently to understand it as a whole.

We also acknowledge that the researchers who performed the thematic analysis have a primarily security and privacy background, whereas most participants did not, and that this difference in experiences may have affected the interpretations the analysts generated. To address this, the researchers took special care to faithfully organize and describe the phenomena our participants described, and to conduct the analysis process with these differences in mind.

4 Library IT staff roles and responsibilities

Before describing the findings of our thematic analysis, we first report descriptively on the roles and responsibilities that library IT staff reported to us. Library IT staff provide a wide variety of digital services to their patrons, and the IT staff participants we spoke with are responsible for making sure those services are functional. Many participants described a responsibility to minimize the security and privacy risk these devices pose to patrons.

Public PC management A near-universal responsibility of our participants was to manage public-facing PCs. Participants reported that patrons use these PCs for recreation, but also for serious and essential tasks, in line with prior findings (Section 2).

> P11: "...they're just going to sit somewhere upstairs all day and watch YouTube and Facebook."

> P12: "Our older patrons tend to use it to do research or read emails, print information. Print forms. A lot of people having been using them for tax information over the last couple of months."

In addition to traditional stationary PCs, some libraries also loan out laptops for individual use, particularly when impacted by COVID-19 closures. Library IT staff are typically also responsible for managing these laptops, which can come and go from the library.

Several participants describe setups where public computing infrastructures are, in fact, run by local or city government or even a vendor, leaving library IT staff with little direct control of how these systems are managed.

Print, copy, and fax management Printing, copying, and faxing are crucial library services. The basic functioning and administration of these services is another key component of what our participants say they do from day to day. Notably, despite reliance on outside vendors, participants expressed less concern about patrons' privacy in this realm.

Libraries handle printing processes in a variety of ways. For example, some libraries use vendor-provided tools to allow automated printing and payment:

> P10: "[Envision, a third-party vendor, has] a print vending system that ties into—we've got like a coin and bill acceptance machine for paying...so somebody could send a document from home or from their phone whatever and come to the library and print it out."

Others use more ad-hoc methods, like a public email address to which patrons can send attachments, which then requires a librarian to manually print (and therefore have access to) their document:

> P12: "Right now, there's only one way to print and what you can do is email your job as an attachment...to the email address we provide...and the subject line has to say print so that it will go into our print folder and get filtered into that."

Managing access to digital resources Libraries often contract with third-party vendors to provide digital resources, like ebooks or access to academic journals. This naturally saves time and effort, compared to developing these materials in-house. However, some participants described privacy concerns relating to the relationship between these vendors and the library's patrons, which we will discuss in detail in Section 5.3 below.

Providing digital skills education Participants say they occasionally provide digital skills education to their patrons, either through open office hours or scheduled events. These cover topics from using common software suites and Microsoft Office to basic online safety. P07 spoke about a more specifically privacy-focused class that ranges from basics to more advanced concepts, which was (perhaps surprisingly) the only class of this sort described by our participants:

> "We have a much more in-depth class that we call "online self-defense" which we start out with the basics and then go all the way up to like, using a secure operating system and stuff like that."

Assisting with day-to-day troubleshooting Some participants say they are also accessible to the public on an as-needed basis. This was sometimes described not as a part of their official job description, but rather a responsibility that arose organically from the needs of their patrons. Circulation staff—who are publicly visible to patrons by the nature of their position—will often receive technical support questions, and when they are unable to answer those questions themselves, will refer the patron to library IT staff. Different participants' libraries dealt with these support requests in different ways, ranging from deliberately arranging computers to be visible from the circulation desk (so that circulation staffers could keep an eye on both), to ad-hoc solutions, like simply flagging down the nearest IT staff member, regardless of what they were previously doing. In most cases, the official role of library IT staff is to maintain library infrastructure rather than provide public-facing tech support, but in practice, they are often asked to provide this support anyway.

P02 experienced both of these strategies, describing technical support questions interrupting their more formal IT work:

> "At this point, the only time I have any interaction with patrons is when I am doing stuff in the lower-level tech center... last week I was imaging some computers down there that weren't being used by patrons. And so, you know, maybe one of the patrons will try to have a conversation with me [for tech support], or one of the librarians that are stationed down there will take this as an opportunity to have me help them help a patron."

However, this participant also indicated that before the pandemic lockdown, they used to run three to four hours a week of dedicated technical support desk time.

5 Findings

In this section, we report on library IT staff members' goals and values, and the threats they described facing. After outlining those individual factors, we describe tensions our participants highlighted between those factors, as well as the constraints that limit their ability to achieve their goals. We use Sen's capabilities approach to frame our findings about how library IT staff think about their patrons' use of library technology and the tradeoffs they make with regard to security and privacy.

5.1 Goals of library IT staff

Participants describe several high-level goals related to library IT, several of which concern the security and privacy of their patrons. Library IT primarily focus on ensuring the capabilities of their patrons to access information, social services, employment, etc. Doing so requires that they provide a trusted space for accessing economic resources and other information in ways that coincide with Sen's notions of capabilities to social opportunities (e.g., education, healthcare) and protective security (including protection from poverty and incarceration or deportation) [54]. Privacy is seen as primarily a way of shielding patrons from surveillance (or the fear of it) by government institutions [54].

Population	Count
LGBTQ+ people	10
People with disabilities	10
Individuals without permanent residence	10
Low-income communities	9
Racial/ethnic minorities	9
Older adults	9
Individuals with a criminal history	8
Low-income single mothers	8
Undocumented immigrants	8
Political activists	5
Journalists	3

Table 2: Patron populations reported by our participants.

Making libraries a safe and trusted space We see this dedication to patrons' capabilities in our participants' goal of making the library a safe and trusted space where patrons can be free to seek information without fear of surveillance by government institutions. This accords with other scholars' views of ICTs as information resources ("making information available and facilitating interaction") that are fundamental to Sen's capability to choose [28]. In this case, providing a safe and trusted space supports this capability.

Our participants frequently explicitly identified libraries as the last remaining trusted public organization/resource in their community.

P04 says, "We are the most trusted institution of any [local government agency]... routinely, in poll after poll we are shown to be a beloved institution." This belief is supported by studies from the Pew Research Center indicating that patrons in the United States view libraries as helpful for finding trustworthy information and making informed decisions [26].

A few participants emphasized the need to maintain the trust of patrons, especially those from populations who might experience higher digital-safety risk. Participants mentioned examples like LGBTQ+ youth, populations who are disproportionately targeted by the police, and people with low socioeconomic status, as patrons who, participants felt, particularly depend on the library for critical information and resources. Almost every participant described serving various such populations in their libraries, as detailed in Table 2. According to participants, protecting these at-risk users' privacy is key to maintaining their safety as well as their trust.

> P05: "There are a lot of LGBT youth who grew up in very conservative household[s] who could have never

searched for that information about who they are, without going to the library. [The library] provided them an avenue and a space to search for information without their parents, knowing or without anybody else, knowing what they were looking at."

P08 described a different concern with retaining the trust of immigrants and undocumented people, where the library itself was seen as a potential adversary that threatened the capabilities of their patrons to live in the U.S. without fear of surveillance or deportation. Framed in terms of capabilities, this participant believes this mistrust (i.e., the chilling effects imposed by fear of being surveilled and deported) interferes with the capability of their patrons to achieve wellbeing through access to resources they use for information seeking and employment:

"[Patrons are] essentially saying 'We're not going to sign up for a library card because this information [their library activities] is going to be sent over to the city government and once it gets sent over to the city government, then law enforcement officials might have access to it.' "

This participant clarified that their library system did *not* share browsing data or other patron information with law enforcement (especially U.S. Immigration and Customs Enforcement (ICE)).

"We do not release information to government officials unless they have a signed judicial warrant, not an administrative warrant the ones that ICE likes to serve people. It has to be a court-issued warrant or subpoena."

However, P08 also indicated that communication around this issue was a challenge, suggesting that it was not unreasonable for patrons to worry that the library, as part of city government, might have an obligation to share data with law enforcement. Despite their efforts to guard against infringements of their patrons' capabilities, the bureaucratic configurations of the system had chilling effects.

"Patrons rightly are not very sure what we exactly do... We are part of the city government, but the way that [the library system] works is that we are separate in terms of hierarchy, we answer to the library board and not straight to the mayor. Our IT systems are separate, meaning that the library IT department has control over the network, has control over the public computers, has control over the Wi Fi network. City IT does not get any of that. So they can't come in and... sniff traffic."

Maintaining library values within larger IT systems Several of our participants—particularly those who worked in smaller towns and cities (and thus in smaller library systems with fewer resources)—described being dependent on local government IT departments to maintain or manage library IT. A few described conflicts in this relationship. P07 describes how the city's IT department, not understanding the library's mission of staunch protection of "patron privacy and intellectual freedom," would use monitoring software to monitor patrons:

P07: "Initially when I was hired, the city IT actually took care of library IT needs, but... there was a lot of conflict there. They did not have a good understanding of the library's mission and they would often do things that were contrary to our library's mission and values... They had monitoring software on the public computers... and they would sometimes observe what the patrons were doing because they thought that it was necessary to make sure that the patron didn't violate our policies. In a corporate IT setting that's perhaps reasonable, and corporate IT may need to monitor employees to make sure they aren't violating corporate policies, but that is directly in contradiction with library values—patron privacy and intellectual freedom."

This participant later noted that "It's easier to teach a librarian IT skills than it is to teach an IT person library values," referring to the need to preserve "patron privacy and intellectual freedom." Library IT staffers' dedication to privacy and intellectual freedom reflects their concern that patrons' capabilities—freedom, in Sen's framework, to make choices to advance their own wellbeing—are infringed upon when those patrons are surveilled (especially in ways that home computer users would not be subject to) reducing transparency and creating distrust.

Availability and usefulness of computing services Another goal of library IT staff members was to support and improve patrons' capabilities by ensuring that use of computing resources was easy, and that patrons could accomplish their goals using library resources.

One component of this goal is making access to public PCs and other infrastructure simple and painless. Most participants described systems wherein participants needed only a library card, or even a guest pass for those without library cards, to use library public computers. P10 described fully open access to their library's computers—patrons only had to sit down at the computer to use it, without any login procedures. This fully open access was an exception, rather than standard practice across our participants.

This goal also manifests in a desire to help patrons accomplish their goals. This was mentioned explicitly in the context of formal and informal tech support, and described implicitly when discussing services like public PC use and printing, which exist to support patrons' needs and capabilities.

Privacy of patron data and activities Most participants described protecting the privacy of patrons who use library IT resources as a core goal.

One near-universal approach was to ensure that patron data or activities are not retained on a public PC after the patron is finished using it, under the theory that if no data is kept, then it cannot be revealed or abused. Participants described wanting patrons to feel comfortable enough with privacy to use library equipment (supporting expansion of capabilities) and also expressed concern about the potential consequences of storing data that could be used against the patrons (limiting capabilities).

> P06: "In principle, I like the ability for somebody to use the internet anonymously without a paper trail if they want. I think that that's a good thing to offer."

Mechanisms for preventing data retention vary across participants' organizations, based on available tools, financial resources, and knowledge. In particular, participants cited vendor software, such as Deep Freeze—a software solution that allows computers to be automatically restored to a default image[3]—as well as OS-level features, like Windows 10's unified write filter (UWF),[4] as primary strategies for ensuring that public terminals are kept in their original state. P02 described using a FOG Project[5] server to manage this need, since it is open-source and thus not a financial drain on the library. However, this method requires significant setup time and maintenance of physical infrastructure, as well as the knowledge to seek out and implement an open-source solution. Participants noted that these data retention protocols are broadly similar for both stationary computers and loanable laptops.

Whether or not patrons must log in (e.g., using a library card number), participants emphasized that they do require patrons to begin and end sessions, in order to protect data when the patron signs off. However, a number of participants lamented that patrons do not log out appropriately, and so in addition to messaging on the computer reminding them to sign out, they have staff provide additional monitoring to ensure that computers are wiped between uses:

> P07: "When they're done, there's a button on the desktop that says 'log out securely.' We also have staff that walk around and if they see something up, then they will hit that 'log out securely' button, which basically wipes out the entire session—any documents, any downloads, any browser history goes away."

Library staff thus ensure that patrons' privacy is consistently preserved.

[3] https://www.faronics.com/products/deep-freeze/enterprise

[4] Unified Write Filter is a Windows 10 operating system feature that redirects writes to the drive to a virtual overlay. This virtual overlay is typically cleared during a reboot or when a guest user signs out.

[5] https://fogproject.org/

Security of library infrastructure One might assume that protecting the library's digital infrastructure—public computing but also other resources, like administrative computers for library staff or printing systems—would also be a key goal for library IT staff. In fact, few of our participants actively mentioned this goal as a high priority, as we will discuss further in Sections 5.2 and 5.3 below.

Indeed, P02 is an exception, noting that Deep Freeze serves two functions: protecting patron privacy, but also "lock[ing] down" the public-facing terminals to prevent tampering, suggesting that other patrons might pose a threat:

> "We do have Deep Freeze on there to reset everything. There are very few permissions on . . . you can't even change the wallpaper, so we try to lock it down as much as possible. We try to make sure everything is wiped off when they get off so that nobody has access to their information."

5.2 Threats faced by library IT staff

We have just described the ways in which library IT staff support patrons' freedom to access information and resources. In this section we discuss several threats they faced when aiming to achieve their goals and responsibilities which we detail below, noting that the the biggest come from outside their walls. That is, library IT staff view the greatest threats to patron's capabilities as institutions like governments and third parties.

Attacks from patrons When asked about security and privacy concerns, participants rarely mentioned their patrons posing any malicious or intentional security or privacy risk to the library or other patrons. Some pointed out that when patrons do create risks, it's most often unintentional.

P06 and P09, for example, noted that problems are rarely caused by malicious users, but that patrons can unintentionally disrupt library computers by accidentally downloading malicious or undesirable software:

> P06: "I don't often deal with people here who I think would do anything maliciously, but it's like they screw up and download something that then slows the computer down or so[mething]."

> P09: "I guess my biggest worry would be, you know downloads. . . They [patrons] click something bad, download something. . . that's probably what I would worry about the most, someone doing something bad unintentionally rather than someone coming in and plugging in a keylogger or whatever."

However, participants are still aware of some potential attacks—P12, for example, described watching for keyloggers as a possible threat. However, they also noted that they doubt that it would be possible to run one on their computers:

P12: "You can't download anything to the computer and save it there. So unless there's a way to have a key logger running in the background of a computer that is not running... I don't know how anyone would be able to do it."

Ransomware attacks One specific attack mentioned by a few participants was ransomware, which is a comparatively common attack on libraries [13].

As P09, who has done advocacy work with several libraries, said, "It's probably every other week that libraries get hit by ransomware." P09 also relates this to patron behavior, as ransomware is usually delivered in this context by clicking on a suspicious download link on the machine in question. However, only one of the five participants who mentioned this attack had actually experienced it, and their PC restoration system was able to solve the problem via a restart. Other participants who discussed this attack mentioned either hearing about it in the news or from colleagues from similar libraries.

Data collection by third-party vendors Several participants expressed concerns about third-party vendors (e.g., ebook providers) having access to patron data. Participants typically described this as a general threat related to their responsibility to protect patrons and their capabilities, rather than citing any specific threats or past incidents with any particular vendor. Participants generally felt ill-informed and ill-equipped to fully understand or counteract threats from third parties.

For example, P01 describes their concern about patrons being required to give personal data to vendors, and how libraries are mostly powerless to enact change:

"With these vendors there's various kinds of data sharing to like, big corporate entities like Amazon. It's a really wild environment and I think it is a great concern. We don't have any meaningful collective negotiating power around it to say no to these practices."

P12 expressed frustration that few vendors hold the same values that libraries do and that libraries are often forced to work with such vendors regardless of this mismatch because of the services they offer:

"We're [public libraries] trying to just provide the information you want and not pry, but a lot of the third-party apps don't seem to care about that. It's frustrating because they're more interested in how much money they can make and that's not really our objective. A lot of the time they'll put together records of what customers are interested in to make really good targeted advertising and are refusing to stop because it's not like there is a library-friendly corporation out there that wants to give us their ebooks. You have to work with a lot of these big monopoly companies and their software so they can do whatever they want."

P08 describes a similar sense of powerlessness: trying and often failing to better understand third parties' privacy practices and potential threats:

"I just read a lot about privacy policies. I read about privacy policies and vendors, their reviews. I also read about vendors' relationships with privacy and public computing, but I don't find that much information."

P08 lamented that not only are libraries unable to prevent existing third party vendor privacy incursions, but the influence (and associated surveillance) of third parties continues to increase:

"We as a profession really don't have a handle of data privacy and security that we should have, especially with ... this exponential increase and working with vendors to provide critical services... And those vendors consolidating and on top of that coming up with new ways to track and surveil our users.

Data requests from law enforcement A few participants defined the goal of patron privacy explicitly as defense against law enforcement data requests. Library IT staff perceive that protecting their patrons from law enforcement supports their capabilities to freely access library resources, whatever their specific goals.

P06, for example, explained their library's data collection policy (with respect to patrons using public PCs) explicitly in terms of how their library's goals (to protect the privacy of patrons) differed from those of law enforcement.

"Our highest concern is our patrons' privacy, it's not serving the police or solving crime, we have different goals... [When] they started saying that they could come in and get your list of patrons or take computers, is when public libraries generally stopped having lists. I wouldn't argue that's coincidental. I think librarians looked at the situation and were like, 'Well, what can we do in this situation to protect the privacy of our users?' The answer was to stop keeping lists because we can't be forced to give them something we don't have."

This threat relates to the goal of making libraries a safe and trusted space (Section 5.1)—P02 described patrons worrying about law enforcement being able to gain records of their activities or information about them. Participants recognize that to support patrons capabilities, they must protect patrons from fear of surveillance, and that doing so requires transparency: they cannot hand over records they do not have. This accords with Sen's notion of transparency as a means to build trust, and to proactively ensure that trust cannot be abused.

5.3 Tensions among goals and responsibilities

Our participants communicated several tensions among their goals and responsibilities, where library IT staff must make choices among competing priorities. We found that library IT staff almost always prioritize capabilities of their patrons over possible threats to the library itself (e.g., allowing anonymous logins to provide patrons with the freedom to search for information without surveillance, even at the risk of not being able to identify threats). The situation is more complicated when different types of patron capabilities appear to conflict with each other (e.g., the capability to access and use services fluently compared to the freedom to so without surveillance. We find that library IT staff are making nuanced decisions about balancing these tradeoffs, grounded in their patrons' needs and experiences.

Patron privacy vs. security of library infrastructure In some cases, ensuring patron privacy can be at odds with taking maximum precautions to protect the security of library infrastructure. For example, libraries could choose to install monitoring software in order to detect misbehavior, or enforce strong login requirements in order to attribute any problems to particular users, but monitoring and logging inherently poses a threat to privacy by tracking user activities.

Our participants almost always prioritized protecting patrons' privacy rather than protecting library infrastructure. P02 describes their library regularly checking hardware for tampering, as well as having security cameras to monitor the physical machines, but notes that such security cameras are unable to view the computer displays so as to preserve patron privacy.

> "We have security cameras but they're not fixed onto the displays of the computers and they're not that detailed anyway. More for like a macro shot. The librarians after a session will see if somebody left anything in the computer, like a USB flash drive left in there. They'll just take it out and put it in Lost and Found."

Similarly, several participants said that their libraries allow anonymous (or near-anonymous) login to public PCs, potentially at the cost of not being able to attribute misbehavior to specific users. The means for implementing this access vary. While many libraries do require patrons to enter their library card number and a PIN in order to begin using workstations, some also allow visitors without a library card to obtain a "guest pass" with temporary credentials for PC usage.

Other participants from university libraries reported that they generally require patrons to log in via their university's central identity management service to access most PCs, but that they do reserve a few PCs with limited services for general access without requiring university credentials.

Other libraries do not require any login at all, and simply present terms of service that users must agree to in order to use the public PC, as P07 describes:

> "If it's a desktop computer, they can just sit down and use it. We have no sign in process or signup process."

Notably, these login decisions also prioritize availability and usefulness of computing services—another way of supporting patrons' capabilities—over security of library infrastructure, by making it easy for people to use the public PCs without extensive signup or login procedures.

Patron privacy vs. availability and usefulness of computing services In other cases, the goals of patron privacy and availability/usefulness of computing services come into conflict, mirroring well-known tradeoffs between confidentiality and availability in other contexts [22]. Measures taken to protect patron privacy from third-parties and law enforcement can create new challenges for patrons, who are unable to store data for later reuse. For instance, one participant describes a patron losing all their documents because they did not realize that anything "saved" to the computer would be erased at the end of the session.

> P04: "Patrons are not always aware of how obsessed with privacy library folks are, so what happens is they will save their resume to the to the desktop, not understanding that when their session ends [it is deleted]... I remember a situation where the person had just saved it there. They didn't ask for the time extension before it ended, and so she lost everything so she had to start all over."

This demonstrates that, if library IT staff's efforts to ensure patrons' freedom from surveillance are confusing or unclear to patrons, they may hamper other patron capabilities.

Relatedly, libraries often block software downloads to protect patrons' safety, which means that patrons don't get the same rich user experience that individuals who own their own PCs would:

> P05: "People can't download anything, they can't add an extension to their browser, like if they were at home. It's kind of locked down... it's a subpar user experience."

These restrictions can also limit patrons' access to critical modern social and work-related activities. For example, P02 described a patron who wanted to use the developer software Xcode, presumably for work or education, but it was not supported on the library's current version of the MacOS operating system. P02 was wary of providing an upgrade, in case the updated OS was not compatible with their security software, Deep Freeze:

> P02: "A patron came up to me and they were using one of our iMacs and they wanted Xcode, but all the iMacs

are running High Sierra and didn't support the current version of Xcode off the App Store. You'd need to do a full update of the operating system and I wasn't able to do it for them at the time, because of how much time it would take, but also because I'm not sure how much compatibility Deep Freeze would have with the newer versions of Mac."

In each of the above cases, libraries opted for privacy and security over availability: limiting some capabilities associated with work, education, or flexible use of computing resources. In these cases, library IT staff placed higher value on freedom from surveillance. Several participants noted that while patrons do express frustration with this situation, they accept it as a necessary condition of using library resources.

In other circumstances, library IT staff make the opposite choice. For example, the print-via-email-attachment mechanism described by several participants (Section 4) prioritizes availability and usefulness over privacy. As P04 points out, sensitive data is sent to their branch email address.

P04: "[A branch email address is] set up to get attachments from the public. And then we print them... it's usually pretty sensitive, you know, like a woman yesterday had tax returns."

Despite the sensitivity of these printed materials, P04 indicated that they did not consider *themselves* as a potential source of privacy violation:

P04: "I don't want to be like the doctor who has seen enough naked bodies, but we see a lot of tax returns. It doesn't really faze me anymore."

This tension between privacy and availability is particularly acute in cases where patrons do not have personal computers at home, or cannot safely use them for sensitive tasks. If these patrons cannot cannot usefully take advantage of library resources, their capabilities will necessarily be limited. Choosing between privacy and availability risks reifying privacy as a "luxury commodity" [43].

Relatedly, P05 worries that simply not having a computer at home—thus making internet use less routine—limits patrons' ability to anticipate or guard against risk:

"If your only computer experiences at the public library... it's more likely that you don't have a computer at home. Or if you're there using the WiFi regularly, you might not have internet at home. And so it's just probably likely that you have less tech knowledge. And so you're not really necessarily thinking about the danger mechanisms or threats."

Other participants reported struggling to inform patrons about risks to their privacy, despite the tools and strategies they had in place, especially when patrons have important competing priorities. For instance, P04 described patrons' needs to complete essential tasks, despite potential privacy risks:

"It gets very tricky, because like if you're doing your taxes... what I consider sensitive, [the patron] may not."

5.4 Constraints of library IT staff

Participants report that their ability to achieve their various goals in support of patron capabilities is also hampered by several constraints that are common across institutions, including reliance on external vendors; limited resources, staff, and training; and outside decision-makers. Here the desire to protect patron's capabilities is undermined by library IT staff members' lack of political and perhaps technical clout.

Library staff rely on external vendors Vendors hold a significant amount of power when it comes to the relationship between vendors and libraries. As P01 notes, libraries are not in a position to negotiate with vendors who, for example, provide funding support for the American Library Association:

"We don't have meaningful collective negotiating power ... to say no to these practices, and part of the reason we don't is that the American Library Association is, like, captured by the vendors, so they are too afraid to take a meaningful stand because they don't want to alienate the vendors who helped fund their twice-yearly annual conference."

This imbalance in power places libraries in a difficult position—they have to choose between keeping their patrons' information out of the hands of vendors (who may not prioritize patron privacy), or tolerate the vendors' collection behavior as the price for providing critical services.[6]

Libraries have limited financial resources Participants describe a lack of (or uncertainty around) financial resources, hindering their ability to implement their IT goals. P11 has had their budget cut to zero:

P11: "My IT budget is zero. Like the line item literally says zero for it. So everything I have to do, I have to do either free, or I just ended up paying for it myself and not telling them."

Some specifically noted challenges in purchasing essential privacy software like Deep Freeze.

P05: "More libraries in the last five years are getting over to [Deep Freeze], but again, it costs money. If you're a small library, you know, it's probably not as available as an option to you."

[6]The ALA's Library Privacy Guidelines for Vendors [1] provides some guidelines for how libraries should choose and manage third-party vendors, emphasizing privacy as a core value.

In the face of limited resources, participants report having to sometimes compromise on their goals and values. For example, P06 discussed implementing web filtering—in their opinion, a form of undesirable censorship—in order to obtain federal grant money, which was needed to maintain high-quality internet service.

> "When we brought fiber into the building, the only way for us to do that was to get federal grant funding, which then requires us to filter to some extent. That was something that I did not do for a very long time, because I have a philosophical issue with it. I don't like it, I wish we didn't have to do it, but the internet service that we [were previously] getting... we couldn't afford it. It was a choice, like, do we take the grant funding and do some basic level of filtering so that we can provide internet for our community, which is so important now? Or do we keep it unfiltered and have terrible service, which, you know, does affect our community."

The lack of resources, therefore, exacerbates the tension between availability and usefulness of computing services and other goals and values.

One participant explicitly associated budget cuts (and therefore a smaller IT staff) with transfer of IT responsibility from the library to the city, noting that the city's use of software-as-a-service and remote servers also reduced their workload:

Library IT teams are often small We learned from our intake survey that half (6 out of 12) of our participants have teams of three or fewer people dedicated to IT at their libraries—including three participants who don't have *any* staffing support besides themselves. Two participants (one who works for a major U.S. city's library system) said they worked in teams of 15–20 dedicated to an entire library system, rather than one branch. In one surprising case, the participant we spoke to was both the primary IT provider for their library and the library's director.

P09 explicitly linked small teams—often a function of the limited resources previously discussed—to decreasing ability to protect patrons.

> "Especially now that there's cutbacks, they just don't have the people and the resources and the know-how... And I do kind of worry that that means there's less focus on IT, and there's going to be fewer people, and things aren't going to be done, things aren't going to be updated. No one's going to be paying attention to the network and things are going to be less safe and secure at these places."

Library IT staff often do not have formal security training Several of our participants describe either themselves, their coworkers, or their supervisors as coming from primarily non-technical backgrounds. This hampers their ability to identify and implement technology that could mitigate surveillance, provide better privacy, enable ease of use, and/or reduce costs. P03, for example, started as a circulation assistant at their university, and eventually came to work there full time as an IT staff member, but did not pursue a degree in computer science or information technology.

P04 indicates that they have little understanding of how the infrastructure works because they have not been trained:

> P04: "To be honest, I don't fully understand the tech infrastructure that we are utilizing. There's no effort made to educate me on it."

This is, in part, because the library administration does not necessarily prioritize technical qualifications when they employ IT staff, and because personnel with both library and IT qualifications can be hard to find:

> P02: "The way they hire people is a little bit strange. Like the way they hire library technical assistants, for example, you don't need any IT credential. They can have library technical assistants that are just like, library-centric, and then library technical assistants that are just IT-centric."

Only one participant, P08, reported having formal education in both library science and IT, via a library degree with an IT concentration. However, P08 noted that this background is unusual, and that a lack of similarly trained professionals (which, according to them, seems to be the norm) hurts libraries' ability to achieve their privacy goals:

> "Individual libraries... don't have the resources to have a privacy person... dedicated privacy trainers or data governance... I'm also seeing a whole number of libraries who are struggling with privacy issues, and there are a lot of gaps that are being filled by some people in the profession, but there's not many people who are dedicated database privacy and security folks."

Library IT staff can be limited by outside decision-makers Participants note that sometimes those making decisions about technology that affect patron privacy and ease of access are not familiar with the library or deeply knowledgeable about how it operates. As a result, changes made for the sake of security are not always in line with patron interests and capabilities, and IT staff are then left to deal with the resultant frustration that patrons experience.

For example, P06 described the administrative bodies responsible for purchasing system upgrades' lack of engagement with patrons' day-to-day challenges as a barrier to availability and usefulness of computing services, especially when updates disrupt tasks and interfaces that patrons are accustomed to:

P06: "Most directors are fully administrative. And so I think sometimes directors or IT managers might not consider the same things I do, because I'm the one helping the patrons, so I know what a pain that's going to be if Windows decides that, what was the version where they decided to put the start menu in the upper right hand and some of the lower left? It was horrible, you had to explain it to every single person that used it. I think, when it comes to upgrading public stuff... I think very hard about that."

P01 notes frustration with administrative bodies comprised non-librarians and people without strong commitment to the library:

P01: "Most of the people who are in library administration are not librarians and [in] that mindset. A lot of them, they're like MBAs, and even worse, like the library board is usually a bunch of local real estate developers who just want to pad their resumé. They don't actually use the library, they don't really understand how it functions."

P02 says that decision-makers who are out of touch also don't know how to make staffing decisions that could better support their goals and resource constraints:

P02: "If they hired a real IT tech, they could just handle everything here for a much cheaper cost, but maybe they're just scared of that. A lot of the administration in the library doesn't really understand technology too well."

Library decisions and policies are also sometimes determined by city or county government and their centralized IT staff. P05 described how this can cause tensions in priorities and values:

P05: "If you're not a large library, your IT is probably the city's IT department, which makes it really challenging because they don't understand libraries... [County name] County's IT staff doesn't really have an understanding of how libraries work and you know, if the manager doesn't really care, the staff isn't going to really care to learn."

6 Discussion

In this section, we explore Sen's concept of capabilities and discuss larger themes and takeaways from these results, particularly around high-level goals and conflicts with other resources and stakeholders. We echo those in the Privacy Enhanced Technologies (PETs) community that have called for a systematically nuanced approach to understanding people's context, freedoms, values, motives, and abilities, advocating for a departure from an idealized usability approach to a capabilities approach [16].

6.1 Sen's capabilities applied to library IT

Sen stipulates that a community should define their own capabilities. In the context of our study, we agree with Sen that capabilities are most usefully defined by those who have insight into day-to-day library activities, including the nuances of what patrons want and need from library IT resources, and library IT staff are often well positioned to do so. We therefore allow our participants to define those capabilities, rather then using an existing framework like that provided by Nussbaum [41]. We find that library IT staff take a contextual or intersectional approach to supporting their patrons [39]: recognizing, for instance, that mitigating surveillance concerns can be highly valued capabilities because they support other sets of capabilities like freedom to access information for employment and social services, etc.

Like Sen, library IT staff think about capabilities both as negative rights (e.g., protection from police surveillance) and as positive rights (e.g., access to coding software that would allow them to perform their job) [52]. Library IT staff perceive that information freedom is tied to privacy guarantees; while those freedoms are articulated through different capabilities in different contexts (e.g., anonymous logins, non-city-dependent IT infrastructures, etc.), the relationship between the goal of information freedom achieved through those capabilities and economic, social, transparency and protective security is ultimately clear [54]. We point this out because privacy strategies are not simply ends in and of themselves, but part of a larger strategy toward achieving freedom.

Library IT staff also understand that while access to internet resources is a critical professional resource, access by itself is not enough. Privacy protocols can create a barrier that makes access less fluid or useful (e.g., security and privacy policies preventing patron usage of preferred software), but can also enable security for patrons to engage with internet resources (e.g., obtaining information about sensitive or stigmatized subjects without fear of retribution).

Throughout our discussion, we highlight the specific metrics that are relevant to understanding enhancement of capabilities of library IT patrons and to making recommendations and evaluating them.

6.2 Privacy needs and moral capabilities

Many of the participants were acutely aware of their role as defenders of values: allowing patrons to use internet technologies without being surveilled by the library, other patrons, or outside entities. This role is ingrained in library values, and, as one of our participants told us, these values are more critical (and possibly more difficult) to teach than IT skills.

Above all, library IT staff considered surveillance to infringe on patron's capabilities—such as freedom to find employment and information, or access other critical resources or social services, etc.—and were mostly willing to put aside li-

brary security concerns for this moral objective. Indeed, Sen's moral approach (which relies on the community to adjudicate value [55]) fits our context well because, as we find, library IT staff are most adamant about protecting their patrons from *law* enforcement. This view stands somewhat in opposition to the normative view of Rawls' distributive justice [47,48] and Walzer's communitarianism [61], in that it challenges government and legal institutions and does not necessarily or entirely put faith in fair distribution of goods or the collective good. Rather, Sen's consequentialist conception of justice deeply considers social realities and aims to eliminate injustice [50], to consider value "not by the resources or primary goods the persons respectively hold, but by the freedoms they actually enjoy to choose between different ways of living that they can have reason to value" [51].

Library IT staff are also attuned to the need to provide basic skills and privacy education to their patrons. Both of these services are critical to enhancing capabilities, which are about quality of access to achieve freedoms which patrons value, rather than simple availability of devices. That said, librarians face constraints in delivering on this promise because of external vendors, decision-makers, and limited financial resources, staff, and training.

However, security and privacy measures can sometimes be a deterrent or disappointment for patrons, especially those who use library resources in lieu of home computers. Despite library IT staff's best efforts, these measures can hamper capabilities linked to fundamental economic freedoms, for example when data is erased after a session or when patron's can't install software they need for work or education. This paradoxically conflicts with library IT staff's perception that they have nurtured capabilities in support of economic, social and social security. At other times, library IT staff prioritize providing easy access to PCs, as if they were patron's own, even when this introduces privacy concerns, e.g., when patrons send their tax information to library email addresses to access the printer. Library IT staffers essentially must make nuanced assessments about which structural threats to privacy are (not) severe enough to warrant limiting other useful capabilities.

Recommendations: Computing researchers and software developers should consider how to create better affordances that can support security and privacy while still allowing people to have an experience on public computer that is more comparable with personal devices. For instance, libraries might offer the ability to run virtual environments on their PCs for patrons that want to use Zoom, Xcode or other unsupported software.

Library staff should be more explicit about their strategies and the tradeoffs they make when considering patrons' privacy. To better socialize the idea that devices are/should be used as impermanent tools, library IT staff should, at very least, put signs on the computers to indicate what data will be erased and why. Additionally, libraries might consider ways to offer printing that might better balance access and privacy. Building on Sen, we also recommend that library IT staff measure the success of these interventions based on how they are valued by patrons, once patrons are informed about the rationale [42]. For example, a metric for gauging the value of Deep Freeze might be to understand if more patrons use computers or use them for longer once staff provide context for Deep Freeze.

6.3 Values in conflict with resources, decision-makers, and other institutions

While avoiding monitoring and not requiring logins are essentially free, library IT staff must sometimes invest in software to ensure that patrons' data is never stored, and this can sometimes create barriers. For libraries with more funding, software enables them to do this quite easily—though, as some mention, they must remind patrons to sign out of computers to ensure that they do their part. Libraries with less funding may struggle since free, open-source alternatives are resource-intensive and possibly esoteric.

In contrast, protecting patrons from vendors that provide critical services like printing or ebook access may feel out of reach due to lack of leverage, and protecting against malicious threats like phishing or identity theft may feel beyond library IT staff's skill level. In other cases, library IT staff feel constrained by out-of-touch decision-makers (who sometimes consider only superficial access to IT resources, rather than more complex capabilities) from making nuanced tradeoffs in support of their patrons' capabilities.

While the ALA advises libraries on how to navigate third-party vendor selection to choose vendors with policies that better secure patron privacy [1], library activists argue for providing encryption and ensuring that the library is the primary data steward [57]. The latter requires that libraries take on a more proactive role, that library IT staff be more sophisticated, and that vendors be more transparent about data policies. Managing these relationships as the ALA advises is therefore challenging, especially since libraries realistically have few options when selecting vendors.

Recommendations: When library staff are constrained by resources, third-party opacity, or skill level from better supporting patron capabilities—including security and privacy—there is an opportunity for the security and privacy community to provide support. Researchers could use measurement studies to provide some transparency into vendor-provided tools, develop open-source projects to better support library needs with lower cost and less surveillance, and provide more user-friendly interfaces as well as training to help library IT staff in their nuanced decision-making. Further, the security and privacy community has an obligation to develop new metrics that better align with enhancing capabilities: measuring

whether and how security and privacy can enhance amount and quality of IT access when patrons feel protected.

6.4 Future work

This paper primarily discusses the perspectives of library IT staff members in the United States. However, while we did not include them in the final analysis, we did interview two participants that worked in libraries in non-U.S., albeit Western countries. While we believe that the contexts of these two participants' libraries were not significantly different from those presented in this paper, we did exclude them from our findings given that they comprised a relatively small proportion of our participant pool. More work should be done to understand the security and privacy priorities and tradeoffs that library IT staff members make in other countries.

Recommendations: Researchers should seek to capture and convey the experiences of library IT staff members in countries around the world to better understand the international perspective of library IT staff's role in the greater security and privacy community.

7 Conclusion

We spoke with library IT staff members about their privacy and security protocols and policies, the challenges they face implementing them, and how this all relates to their patrons. We found that participants are primarily concerned with protecting their patrons' privacy from threats outside their walls, such as police and government authorities and third-parties, and occasionally from other patrons who also use the devices. Despite their dedication to patron privacy, library IT staff frequently have to grapple with tradeoffs primarily associated with supporting patron capabilities—i.e., providing easy access to internet technologies or third-party resources and protecting library infrastructure while also ensuring patron privacy. These tradeoffs point to opportunities for libraries to offer affordances that better balance patrons' access needs with privacy but may require, as participants suggest, decision-makers who are more attuned with the needs and challenges of patrons, and for privacy and security researchers to develop tools that could help to address these tradeoffs while also fitting within the unique constraints of library systems. For security and privacy researchers, library IT staff provide important insight into what is at stake when we take privacy values seriously, because they oversee an environment that represents a critical intersection between people's access to vital digital resources and fundamental privacy issues like freedom to search for information and seek government assistance without surveillance.

Acknowledgements

We would like to thank our study participants, shepherd, and the USENIX Security 2023 reviewers for their feedback, which helped to improve the paper. We particularly recognize Andrell Rice who inspired this research.

References

[1] American Library Association. Library privacy guidelines for vendors, 2015. https://www.ala.org/advocacy/privacy/guidelines/vendors.

[2] American Library Association. Professional ethics, 2017. https://www.ala.org/tools/ethics.

[3] American Library Association. Access to library resources and services, 2021. https://www.ala.org/advocacy/intfreedom/access.

[4] American Library Association. Resolution on the misuse of behavioral data surveillance in libraries, 2021. https://www.ala.org/advocacy/intfreedom/datasurveillanceresolution.

[5] Julia Angwin. First library to support anonymous Internet browsing effort stops after DHS e-mail. *Ars Technica*, 2015. https://arstechnica.com/tech-policy/2015/09first-library-to-support-anonymous-internet-browsing-effort-stops-after-dhs-e-mail/.

[6] Australian Library and Information Association. Libraries and privacy guidelines, 2005. https://www.alia.org.au/Web/Web/Research-and-Publications/Guidelines/Libraries-and-Privacy-Guidelines.aspx.

[7] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77–101, 2006.

[8] Virginia Braun and Victoria Clarke. Reflecting on reflexive thematic analysis. *Qualitative research in sport, exercise and health*, 11(4):589–597, 2019.

[9] Sarah Brayne. Enter the dragnet. *Logic*, 2020. https://logicmag.io/commons/enter-the-dragnet/.

[10] Sarah Brayne. *Predict and surveil*. Oxford University Press, New York, NY, January 2020.

[11] Kelly Caine. Local standards for sample size at CHI. In *Proc. CHI*, 2016.

[12] Matthew Cantor. US library defunded after refusing to censor LGBTQ authors: 'We will not ban the books'. *The Guardian*, 2022. https://www.theguardian.

com/books/2022/aug/05/michigan-library-book-bans-lgbtq-authors.

[13] Will Caverly. Ransomware attacks at libraries: How they happen, what to do, May 2021. https://publiclibrariesonline.org/2021/05/ransomware-attacks-at-libraries-how-they-happen-what-to-do/.

[14] Patricia Hill Collins. *Intersectionality as critical social theory*. Duke University Press, 2019.

[15] Edward M. Corrado. Libraries and protecting patron privacy. *Technical Services Quarterly*, 37(1), 2019.

[16] Partha Das Chowdhury, Andrés Domínguez Hernández, Marvin Ramokapane, and Awais Rashid. From utility to capability: A new paradigm to conceptualize and develop inclusive PETs. Publisher: Association for Computing Machinery (ACM).

[17] Andrew Guthrie Ferguson. *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. NYU Press, 2017.

[18] Martin Garnar and Trina Magi, editors. *Intellectual Freedom Manual, Tenth Edition*. ALA Editions, 2020.

[19] Christine Geeng, Mike Harris, Elissa Redmiles, and Franziska Roesner. "Like lesbians walking the perimeter": Experiences of U.S. LGBTQ+ folks with online security, safety, and privacy advice.

[20] Georgetown Law Centeron Privacy & Technology. American dragnet: Data-driven deportation in the 21st century, 2022. https://americandragnet.org/.

[21] April Glaser. Long before Snowden, librarians were anti-surveillance heroes. *Slate*, 2015. https://slate.com/technology/2015/06/usa-freedom-act-before-snowden-librarians-were-the-anti-surveillance-heroes.html.

[22] Lawrence A. Gordon and Martin P. Loeb. The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4):438–457, 2002.

[23] Greg Guest, Arwen Bunce, and Laura Johnson. How many interviews are enough?: An experiment with data saturation and variability. *Field Methods*, 18(1):59–82, 2006.

[24] Eszter Hargittai. Second-level digital divide: Differences in people's online skills. *First Monday*, 7(4), 2002.

[25] John Horrigan. Libraries at the crossroads. Technical report, Pew Research Center, 2015.

[26] John Horrigan. Libraries 2016. Technical report, Pew Research Center, 2016.

[27] Anil Kalhan. Immigration surveillance. *Maryland Law Review*, 74:1, 2014.

[28] Dorothea Kleine. ICT4WHAT? - using the choice framework to operationalise the capability approach to development. In *Proc. ICTD*, 2009.

[29] April D. Lambert, Michelle Parker, and Masooda Bashir. Library patron privacy in jeopardy: an analysis of the privacy policies of digital content vendors. In *Proc. ASIS&T*, 2016.

[30] Sarah Lamdan. Librarianship at the crossroads of ICE surveillance. *In The Library With The Lead Pipe*, 2019. https://www.inthelibrarywiththeleadpipe.org/2019/ice-surveillance/.

[31] Sarah Shik Lamdan. Social media privacy: A rallying cry to librarians. *The Library Quarterly: Information, Community, Policy*, 85(3):261–277, 2015.

[32] Amy E. Lerman and Vesla Weaver. Staying out of sight? concentrated policing and local political action. *The ANNALS of the American Academy of Political and Social Science*, 651(1):202–219, 2014.

[33] Monica Maceli. Librarians' mental models and use of privacy-protection technologies. *Journal of Intellectual Freedom & Privacy*, 4(1), 2019.

[34] Mary Madden. Privacy, security, and digital inequality: How technology experiences and resources vary by socioeconomic status, race, and ethnicity. *Data & Society*, 2017.

[35] Mary Madden, Michele Gilman, Karen Levy, and Alice Marwick. Privacy, poverty, and big data: A matrix of vulnerabilities for poor americans. 95(1):053–125.

[36] Alice Marwick, Claire Fontaine, and danah boyd. "nobody sees it, nobody gets mad": Social media, privacy, and personal responsibility among low-SES youth. *Social Media + Society*, 3(2), 2017.

[37] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F. Churchill, and Sunny Consolvo. Stories from survivors: Privacy & security practices when coping with intimate partner abuse. In *Proc. CHI*, 2017.

[38] Nora McDonald and Andrea Forte. The politics of privacy theories: Moving from norms to vulnerabilities. In *Proc. CHI*, 2020.

[39] Nora McDonald, Rachel Greenstadt, and Andrea Forte. Intersectional thinking about PETs: A study of library privacy. *Proceedings on Privacy Enhancing Technologies*, 2023.

[40] Gautama Mehta. Proposal to install spyware in university libraries to protect copyrights shocks academics. *Coda Story*, 2020. https://www.codastory.com/authoritarian-tech/spyware-in-libraries/.

[41] Martha C. Nussbaum. *Creating Capabilities*. Harvard University Press, 2011.

[42] Ilse Oosterlaken and Jeroen van den Hoven. Editorial: ICT and the capability approach. *Ethics and Information Technology*, 13(2):65–67, March 2011.

[43] Zizi Papacharissi. Privacy as a luxury commodity. *First Monday*, 15(8), 2010.

[44] Ruth Pearce. A methodology for the marginalised: Surviving oppression and traumatic fieldwork in the neoliberal academy. *Sociology*, 54(4):806–824, March 2020.

[45] Susannah Quick, Gillian Prior, Ben Toombs, Luke Taylor, and Rosanna Currenti. Cross-European survey to measure users' perceptions of the benefits of ICT in public libraries. Technical report, Bill and Melinda Gates Foundation, 2013.

[46] Lee Rainie. The information needs of citizens: Where libraries fit in. *Pew Research Center*, 2018.

[47] John Rawls. *Justice as Fairness: A Restatement*. Belknap Press.

[48] John Rawls. *A Theory of Justice: Revised Edition*. Belknap Press.

[49] Elissa M. Redmiles, Amelia R. Malone, and Michelle L. Mazurek. I think they're trying to tell me something: Advice sources and selection for digital security. In *Proc. IEEE S&P*, 2016.

[50] Amartya Sen. *Identity and Violence: The Illusion of Destiny*. W. W. Norton & Company.

[51] Amartya Sen. Justice: Means versus freedoms. *Philosophy & Public Affairs*, 19(2):111–121.

[52] Amartya Sen. Rights and agency. 11(1):3–39. Publisher: Wiley.

[53] Amartya Sen. *Capability and Well-Being*. Clarendon Press, 1993.

[54] Amartya Sen. *Development as Freedom*. Alfred Knopf, 1999.

[55] Amartya Sen. *The Idea of Justice*. Belknap Press, 2009.

[56] Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. Computer security and privacy for refugees in the United States. In *Proc. IEEE S&P*, 2018.

[57] Sanhita SinhaRoy. Defenders of patron privacy. *American Libraries: The Magazine of the American Library Association*, 2021.

[58] Joan Starr. Libraries and national security: An historical review. *First Monday*, 9(12), 2004.

[59] Jan van Dijk. *The Digital Divide*. Polity Press, 2020.

[60] Jessica Vitak, Yuting Liao, Priya Kumar, and Mega Subramaniam. Librarians as information intermediaries: Navigating tensions between being helpful and being liable. In *Proc. iConference*, 2018.

[61] Michael Walzer. *Spheres Of Justice: A Defense Of Pluralism And Equality*. Basic Books.

[62] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L. Mazurek, Manya Sleeper, and Kurt Thomas. SoK: A framework for unifying at-risk user research. In *Proc. IEEE*, 2022.

[63] Pamela Wisniewski, Heng Xu, Mary Beth Rosson, and John M. Carroll. Parents just don't understand: Why teens don't talk to parents about their online risk experiences. In *Proc. CSCW*, 2017.

[64] William Wresch. Progress on the global digital divide: an ethical perspective based on amartya sen's capabilities model. *Ethics and Information Technology*, 11(4):255–263, September 2009.

[65] Kathryn Zickuhr, Lee Rainie, and Kristen Purcell. *Library Services in the Digital Age*. Pew Internet & American Life Project, January 2013.

[66] Shoshana Zuboff. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs, 2019.