FEATURE

Patron Privacy Protections in Public Libraries

IT Professionals' Points of View

Authors _ Chieh-Li Chin (cchin6@illinois.edu), University of Illinois at Urbana-Champaign. **Tian Wang** (tianw7@illinois.edu), University of Illinois at Urbana-Champaign. **Erh-Hsuan Wang** (ewang36@illinois.edu), University of Illinois at Urbana-Champaign. **Dr. Masooda Bashir** (mnb@illinois.edu), University of Illinois at Urbana-Champaign.

Public libraries serve as crucial resources for the public to access information, with the safeguarding of patrons' privacy being a longstanding and essential mission. This study builds on a previous survey that delved into the perspectives of public librarians and administrators on patron privacy protection. Our specific goal in this study was to identify the practices employed by Information Technology (IT) professionals and the challenges they face in safeguarding patrons' privacy within public libraries. Conducting a comprehensive focus group study involving 33 IT professionals across 10 sessions, we sought to gain insights into their experiences and perspectives on protecting patrons' privacy. Our findings reveal that IT professionals express concerns about patrons' lack of awareness regarding the significance of privacy protection, placing staff in the challenging position of balancing convenient customer service with the imperative to protect patron privacy. Moreover, a notable challenge faced by IT professionals in libraries is the lack of training and technical knowledge among library staff to optimize technologies for ensuring patrons' privacy. The study also highlights IT professionals' reservations about the collection of patrons' data by libraries or vendors, prompting a desire for a deeper understanding of both technical and nontechnical measures to enhance privacy protection. While our research sheds light on the concerns and practices of library IT professionals, we believe the insights gained can provide library administrators and policymakers to gauge the critical role of technology in privacy protection. By understanding these challenges, policymakers can modify and implement policies and practices to effectively enhance the protection of patrons' privacy in public libraries.

Public libraries are one of the main readily available and affordable resources for people to access information (Real 2017). According to the data collected from more than 9,000 public library systems comprised of approximately 17,000 individual main libraries in the US, Americans made 1.2 billion in-person visits to the public libraries in 2019 (Pelczar et al. 2021) and visited libraries' websites more than 1.1 billion times in 2021 (Pelczar et al. 2023).

Public libraries play a critical role in providing free public internet access (Jaeger and Fleischmann, 2007), and according to the 2020 Public Library Technology Survey Summary Report, 98.4% of libraries continue to provide this service (2021). In addition, the primary technology services offered by public libraries include teaching basic computer skills (82.3% of libraries surveyed), providing access to online health (60.7%), online employment (63.5%), and online language learning resources (53.1%), as well as offering digital literacy trainings on general internet use (82.6%), online databases use (73.4%), and safe online practices (58.1%) (Public Library Association 2021). Specifically, the digital resources and infrastructures provided by the public libraries across the US were essential for many communities during the COVID-19 pandemic to stay connected (Bryne and Visser 2022). While library buildings were closed to the public during the pandemic, more than 60% of the public libraries offered Wi- Fi internet access for people outside of the buildings. In addition, usage of electronic materials and online services had significantly increased from FY2019 to FY2020 given the stay at home or place of residence requirements during COVID-19 (Institute of Museum and Library Services 2023).

Furthermore, the digital services provided by the public libraries have been particularly valuable to and utilized by vulnerable groups such as low-income households, individuals with few computer skills, and those of low socioeconomic status, since they rarely have other options for access to computers and internet services (Vitak et al. 2018). Marginalized groups such as youth, women, and law-income families particularly benefit from public computers, internet, or Wi-Fi connection provided at libraries to seek health information, learn new technologies, discover community resources, find jobs, and gain workforce skills (McCarthy 2020; Horrigan 2015). Nevertheless, vulnerable groups are often at a higher risk of being targeted by increased surveillance or becoming victims of data leakage given their lower digital literacy to protect their private information (Pacific Library Partnership and LDH Consulting Services 2020).

Protection of patrons' privacy has long been a critical mission of public libraries. As stated in the American Library Association's Library Bill of Rights (American Library Association 2019), "All people, regardless of origin, age, background, or views, possess a right to privacy and confidentiality in their library use. Libraries should advocate for, educate about, and protect people's privacy, safeguarding all library use data, including personally identifiable information." Thus, libraries are responsible for providing a trustworthy environment for patrons spanning from the most privileged to the most vulnerable to access information safely (Pacific Library Partnership and LDH Consulting Services 2020). However, as indicated by a recent online survey study conducted during the pandemic (Wang et al. 2023), notable disparities exist in the practices and challenges related to patron privacy protections in public libraries. According to this recent study, approximately a quarter of the survey respondents reported that their libraries do not have a dedicated policy in place to address patron privacy. Moreover, more than one quarter of the survey respondents highlighted a lack of staff training in patron privacy protection, and more than two-thirds of the libraries do not provide educational materials for patrons on privacy protection.

While the Wang et al. study offered valuable insights from more than 700 librarians, library staff, and library administrators, it lacked adequate participation from information technology (IT) professionals affiliated with public libraries compared to other key stakeholders working in public libraries. We believe IT professionals in public libraries play a critical role in managing software and hardware operations, efficiently storing data, supporting staff and patrons in various media and technologies, as well as serving as key consultants in technology expansion. Therefore, their professional perspectives from an operational standpoint prove useful and necessary when studying privacy practices within these spaces. To fill this gap, this study is focused on how IT professionals perceive patrons' privacy protections in public libraries. To gain this perspective, we conducted an online focus group study that investigated IT professionals' practices and challenges as it applies to their day-to-day work to protect patrons' privacy in public libraries. To the best of our knowledge, this is the first study that focuses on IT professionals' views when it comes to patron privacy. Motivated by the results obtained in a prior study that investigated practices and challenges concerning patrons' privacy from the viewpoints of librarians and library administrators (Wang et al. 2023), our research is guided by the following four primary research questions to explore IT professionals' perspectives:

- RQ 1: What do IT professionals perceive as the most pressing concern or challenge related to patron privacy protection in public libraries?
- RQ 2: What technologies or practices do their libraries use to protect patron privacy?
- RQ 3: Of the technologies and services libraries use, what do IT professionals believe poses the most serious challenge to patron privacy?

- RQ 4: From IT professionals' perspectives, what kind of technological changes, if any, should public libraries in general make to better protect patron privacy?

Related Literature

As stated earlier, since this is the first study of its kind, the literature reviewed in this section is relevant to our study while it is not directly comparable. Therefore, the literature reviewed below is focused on the dynamic landscape of privacy challenges caused by technologies and the diverse practices proposed to tackle them, such as 1) the privacy risks caused by technologies in public libraries, and 2) the prior approaches offered to address privacy concerns related to these technologies.

Privacy Risks Precipitated by Technologies

According to ALA's Interpretation of the Library Bill of Rights, "The right to privacy includes the right to open inquiry without having the subject of one's interest examined or scrutinized by others, in person or online" (American Library Association 2006). Recent scholarly publications have highlighted the increased privacy risk associated with the exposure of patrons' personally identifiable information and library-use data. These risks are particularly relevant to the use of technologies in libraries. Noh (2017) conducted a survey reviewing literature on patron privacy focusing on libraries in the United States and South Korea over the past few decades. She found the main themes that had been discussed in the literature were concept of personal information and privacy, libraries and intellectual freedom, policies, guidelines, and laws related to library privacy. In particular, Noh specifically identified that there had been increasing risks of damage to patron privacy caused by the greater use of information technologies in libraries.

Moreover, scholars have called attention to the risks of privacy exposure caused by new technologies. These risks extend beyond the applications patrons utilize on their personal devices, as demonstrated by Sweeney and Davis (2021) in their examination of privacy concerns associated with voice assistants. In addition, the adoption of third-party software within public libraries, such as Axis 360, Hoopla, OneClickDigital, OverDrive, and Zinio (Lambert, Parker, and Bashir 2016), making library patrons' data no longer solely protected in the hands of the librarians and the patrons. Likewise, the advanced smart and digital technologies that library staff and patrons access in the public libraries (Adetayo et al. 2021) can inadvertently compromise the privacy of individuals. It becomes increasingly critical for libraries to navigate these potential privacy concerns which emerge with the advent of the new technologies.

Furthermore, library practices that intended to improve patrons' convenience could also bring threat to patrons' privacy. For example, in order to offer the best services to patrons, libraries have increasingly relied on cloud-based services and big data analysis to properly allocate libraries' funding and resources in the Library 2.0 era (Kritikos and Zimmer 2017; Tella 2019). Particularly, given the restrictions on in-person services during the COVID-19 pandemic, the needs for libraries to provide virtual services also grew. Some libraries chose to accept free content from vendors given their lack of funding; however, this poses privacy risks for patrons and libraries given that this content was not licensed or governed by privacy agreements (White 2021). Utilizing data and technologies to enhance customer experience while protecting patrons' privacy has therefore become challenging for librarians (Asher 2017, Corrado 2007; Harper and Shannon 2017, Pekala 2017).

Prior Studies Related to Privacy Concerns and Technologies

Researchers have proposed various approaches to address privacy concerns created by technologies from differing perspectives. A few scholars conducted real-world case studies for creating policies or best practices on protecting privacy. Marden (2017) shared experience in creating a new privacy policy at the New York Public Library that follows the "Standard Privacy Principles" outlined in the ALA's Intellectual Freedom Committee's guidelines. Yoose (2017) and Loter (2016) examined the practices in the Seattle Public Library that obscured identifiable data of individual patrons. This approach not only protects patrons' privacy but also fulfills the library's information needs of knowing how patrons use the library.

Other literature examined specific new technologies that could better protect patrons' privacy, such as VPNs (McAndrew 2020), HTTPS (Thomchick and San Nicolas-Rocca 2018), and Tor (Lund and Beckstrom 2021). There have also been literature aiming to advance library employees' knowledge of and skills on advanced technologies; for example, Fortier and Burkell (2015) taught librarians the mechanisms as well as benefits and risks of online behavioral tracking technology, further instructing librarians how to evaluate behavior tracking practices and provide patrons digital literacy education to protect their privacy. Henning (2018) wrote a quick guide on voice computing programs for librarians to learn what these computing programs are, how they can be applied to libraries and specific privacy concerns with these technologies. Researchers have similarly introduced frameworks for ethical data practices that apply to future data technologies (Lund 2022). The American Library

Association and scholars also studied libraries' relationship with vendors to advise libraries on how to assess cyber security issues and review license agreements with vendors periodically to secure libraries' data and protect patrons' privacy (American Library Association 2015; Ayre 2017; Caro 2016, Corrado 2020).

Despite the numerous technological and educational approaches that have been proposed to address the privacy concerns related to technologies in public libraries, there are still gaps between the real-world practices and the recommended best approaches. For example, Breeding's survey (2016) on how current library systems address the privacy and security issues related to patrons found only 13% of the large academic libraries and 8% of the large public libraries considered in the survey presented their website using HTTPS. Furthermore, a content and cluster analysis on public libraries' data privacy policies revealed less than 50% of the public libraries sampled had a data privacy policy available online (Lund 2021). A review on libraries' social media policies also indicated the lack of consensus on privacy protection best practices among libraries using social media platforms (Cotter 2016). Prior studies have demonstrated library staff do not have adequate knowledge to operate the privacy-protecting technologies used in the libraries (Maceli 2019) or guard patrons' privacy in their daily practices that could involve in working with patrons' private information (Morehouse et al. 2020). A recent survey indicated library employees consider employee trainings regarding patron privacy protections and resources to help employees gain knowledge about privacy-enhancing technologies as the most-needed solutions for patron privacy protections (Wang et al. 2023). There are undetected or unaddressed barriers preventing libraries from adopting appropriate technologies, recommended policies, and best practices to protect patrons' privacy. Hence, our study aimed to work with the IT professionals that interact with library staff, patrons, and technologies daily in public libraries to identify their practices and challenges in protecting patrons' privacy. To the best of our knowledge, this study is the first that focused on IT professionals in public libraries to explore their concerns, learn practicable solutions, and propose achievable guidelines for the library community.

Methods

This study utilized focus groups to gain insight into patron privacy protection, as perceived by the IT professionals working with public libraries. The focus group discussions were conducted online via video conferencing due to pandemic-related travel and in-person meeting restrictions. This format also allowed us to engage with IT professionals from diverse geographic locations across the United States. We hosted 10 sessions of online focus group discussions using Zoom in the Summer of 2021, and each of the sessions had 2 to 5 participants. The participants were assigned to focus groups randomly based on their availability.

The primary goal of the focus group study is to identify the technological tools and practices employed by public libraries to ensure patrons' privacy protection and understand the challenges IT professionals experience in protecting patrons' privacy. To construct the focus group questions, our research team comprised library privacy experts and Library and Information Science graduate students with prior work experience in libraries. More specifically, the research team collaborated with an advisory board of subject matter experts with diverse backgrounds related to library privacy, including directors of urban and small libraries, independent consultants on library privacy and library technology, administrators from national library associations, the director of the Library Freedom Project, and researchers in the library privacy field. The advisory board reviewed the proposed questions and provided feedback based on their experience working with various sizes, areas, and types of public libraries. Drawing upon a foundation of existing research on library privacy and the latest American Library Association Library Privacy Guidelines, we formulated a series of questions and follow-up inquiries. Following the prior survey that addressed practices and challenges regarding patrons' privacy protections from librarians' and library administration's perspectives (Wang et al. 2023), these questions were designed to answer our research questions from the following aspects: (1) exploring the most pressing concern or challenge related to patron privacy the IT professionals have faced; (2) recognizing the technologies or practices used in public libraries to protect patron privacy; (3) identifying the technologies and services the IT professionals think would pose the most serious challenge to patron privacy; and (4) assessing the potential technological changes the public libraries could make to better protect patron privacy. The focus group study questions and research protocol have been reviewed and approved by the Institutional Review Board of the research team's University.

Data Collection

We focused the recruitment activities on electronic methods given the limitations surrounding the COVID-19 pandemic. A mailing list was compiled to reach out to over 12,500 individuals worked in state public libraries in addition to library association working groups such as IT professionals associated with the Public Library Association

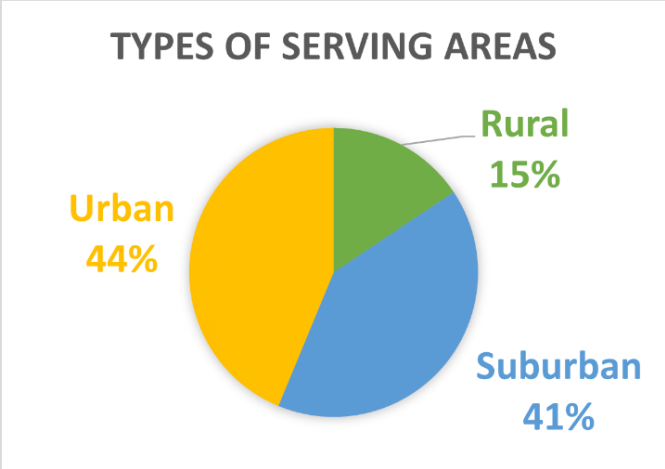

Figure 1. Types of Areas Serving by Focus Group Participants' Libraries

or the American Library Association. We also contacted library associations representing under-represented minorities (e.g., The National Association to Promote Library and Information Services to Latinos and the Spanish-Speaking (REFORMA), the Black Caucus of the American Library Association (BCALA), the American Indian Library Association, (AILA), the Asian/Pacific American Librarians Association (APALA), and the Chinese American Librarians Association (CALA)). The email contained a link for participants to sign up for the online focus group discussion. In the sign-up form, participants were asked to certify that they work on information technologies and are affiliated with public libraries in the US They were asked to provide their name, library affiliations, email addresses, and availabilities for researchers to follow up and schedule the online focus group discussion session that best suited each participant's availability. In addition, the participants were asked to specify whether their libraries are associated with library associations representing ethnically under-represented minorities or serving underserved communities. Before joining their online focus group discussion, participants received a consent form that clearly described the goal, format, and logistics of the focus group discussion. Participants were asked to read and submit consent to the consent form prior to the online focus group discussion beginning. During the online focus group discussion, the sessions were recorded (using Zoom's function) and transcribed for the research team to do analysis. No identifiable information was revealed in the aggregated analysis results. Upon completion of the online focus group discussion, all participants were offered an e-gift card to compensate for their participation.

Table 1. Participants' Occupation

Types of Job Titles	Count
Directors or Heads of Information Technology	7
Managers for IT departments or IT services	11
IT coordinator	3
IT Technician or Specialist	3
Librarians	6
Non-IT Department Heads	3

Study Participants

We identified participants' titles and the types of community their libraries serve by gathering information from their self-introductions during the focus group sessions or through online searches of their names and affiliations. The participants in the focus group study were diverse in terms of the community types they serve and their roles in the public libraries. Among the 33 participants, 15% were working in libraries serving rural areas (n = 5), around 40% worked in suburban areas (n = 13), the remainder worked in urban areas (n = 14) or worked in a library consortium that serves multiple types of communities (see figure 1). Although none of the participants are working in libraries that are directly affiliated with library associations representing ethnically under-represented minorities, 36% of the participants (n = 12) reported their libraries are serving underserved communities.

The majority of these participants were at the administration level in charge of the information technology services in public libraries, including Directors or Heads of Information Technology (n = 7), or Managers for IT departments or IT services (n = 11) such as Integrated Library System Managers. Other participants worked at the front line to interact with information technologies in libraries, including IT coordinator (n=3) and IT Technician or Specialist (n = 3). There were 6 librarians joining the focus group study, 2 of them are technical librarians. Three of the participants were directors of non-IT departments but also needed to deal with information technologies in their day-to-day work (see table 1).

Content Analysis

To analyze the responses in the focus group discussions, we conducted a qualitative analysis to identify text-based evidence through a bottom-up approach (Bernard et al. 2016). For each of the research questions, three researchers were trained by a senior researcher with extensive experience in qualitative analysis to closely read a set of responses and identify the themes or topics described in the text in response to

each of the focus group questions. Based on the themes identified from the first round of annotations, the research team compiled a coding schema to categorize the themes for each of the research questions. The annotators then categorized each response into the corresponding theme. After each annotator coded the responses independently, the annotators convened to synthesize the annotation results and agreed on the category that best describes each response.

Results

RQ 1: What do IT professionals perceive as the most pressing concern or challenge related to patron privacy in public libraries?

The most pressing concerns the IT professionals brought up during the focus group discussions were those related to **using software, applications, and systems**. For example, these library IT professionals worried about how the applications used in the library might track interactions patrons have on public machines. One of the respondents said:

> It is unknown what apps on the computer are tracking which interactions patrons might have on the public machines.

Other participants reported that some library systems have not been updated for many years and do not have the option to encrypt data or send data over SSL ports. For example, one IT professional mentioned:

> One thing that I've still not been able to resolve is we send SIP over unencrypted ports as well, every single check in and check out sent, I don't know who is really trolling that information, you know how big of a concern is it.

Another participant noted:

> ISPs (internet service providers) may be tracking what websites you go to . . . seeing all those transactions . . . it's not encrypted, that's plain text transfer.

Participants also indicated library software that works well for large libraries does not meet the needs of small libraries. Library staff often needed assistance or authorization to configure software features related to patron privacy such as setting up firewall filters or removing facial recognition. A respondent indicated:

> While we specifically avoided any facial recognition tech in the cameras, it's a hardware restriction, or, it may be a built in feature that we're trying to limit with software, we don't really know if the software is properly limiting this or if it's just collecting this data on the back end and sending it out somewhere.

Furthermore, IT professionals working in public libraries were also concerned with their **libraries' practices in managing patrons' data**. They noticed their libraries collect more information than necessary for analysis or lose control of data shared with the vendors and consortium. They worried if data left on paper forms or files left in printing machines were not deleted in time.

Another main concern library IT professionals often shared is the challenge related **to balancing between providing customer service and protecting patron privacy**. They shared frustrations of not being able to help patrons with limited computer skills to enter the patrons' private data, given that this would violate their libraries' privacy policy. For instance, one IT professional said:

> One of the challenges that we're fighting often is that our patrons don't take privacy as seriously as they should, and so oftentimes they're willing to take risks that we, as the library just can't do so. Balancing security with convenience is closely tied to that.

Similarly, another respondent also mentioned:

> Many of the people who come to use our public computers are economically disadvantaged. they may not have the skills to understand cyber security, and I think all of us struggle with rights to privacy versus convenience.

Other concerns reported were responding to requests from **law enforcement**, and the **lack of training for staff and patrons**.

A follow-up question was asked to further explore the concerns these IT professionals have heard from their patrons or their non-IT-pro colleagues. The participating IT professionals were concerned their non-IT-pro **colleagues do not have adequate knowledge and skills in technologies and patron privacy protections**. This concern is related to inconsistent procedures and policies within organizations, or staff having a hard time understanding the culture of the libraries. As one of the IT professionals noted:

> The challenge that I am really having with the staff is the inconsistency of trying to understand the seriousness of patron privacy . . . sometimes it's a workaround. We're having trouble with technology so then they'll just give out the reference desk email address to have somebody send a document.

> But then they're not getting rid of that email that has personal information in it.

In addition, another pressing concern the participants expressed was **patrons lack of technical knowledge and failure to protect their privacy**. For example, patrons found the filter for internet access inconvenient, overshared their information, or left paper forms with private information in public areas. On the other hand, some patrons were aware of the importance of privacy protections and thus cautious about **how their data was being accessed, used, or shared**. For example, patrons questioned whether their data was tracked on wireless services or public computers, worried that others would overhear their conversations with library staff, were reluctant to show their photo IDs or share their contacts with library staff, and suspected whether the government has been watching their data.

RQ 2: What technologies or practices do libraries use to protect patron privacy?

According to the study participants, libraries have often adopted software and hardware to protect patron privacy. For example, several libraries used Deep Freeze or other **session management tools** to wipe out browsing history and computer logs after machines reboot. Libraries have often implemented **VPN, data encryption, and firewall** to protect data transferred online. As mentioned by an IT professional working with library consortium:

> We require every library to use very specific set of firewalls and we have VPN connections to every one of those libraries, that is connected to a staff network, so that ensures at least that level of access is encrypted and that they're talking to our iOS via encrypted method.

Some of the participants also stated that their libraries replaced traditional patron IDs with a **patron barcode system** to avoid accessing patrons' private identifiable information. Furthermore, some participants indicated that the public libraries they worked in have applied proper **data practices** and policies related to data collection, use, access, and deletion that protect patrons' privacy. For example, some methods noted were logging people out and purging records regularly after each session, cleaning printing jobs after each hour, encouraging strong passwords, using encrypted secure certifications, not mentioning patrons' personally identifiable information in emails, and deleting data that was no longer needed. As one of the respondents noted:

> We were using deep freeze on our public computers, in addition to the browser is not storing data in the first place so they're not tracking any reading history . . . deep freeze wipes the hard drive functionally when the machines restarted.

Another IT professional mentioned:

> [For] the Xerox copier we have kept the job encrypted, so it would be reprinted but it's dumped at the end of the night, so those are gone once that happens.

Our study participants also reported that some libraries have conducted **regular privacy audits** and have a locked data center to ensure privacy protection. One IT professional shared:

> For the first time since I've been at my institution my consortium did a security audit, which was really eye opening. For us to see like where vulnerabilities are and it kind of gives you a chance to think about how that might affect folks interacting with us through some of our public channels. We're more aware than we used to be, which is always a good thing.

Some participants stated their libraries would provide staff documentation **and training on security and privacy** to help them gain knowledge on protecting patron privacy. For example, one IT director noted:

> [We offer] continuous training and education for our staff on the importance of the privacy and data." The training could also come from peers, as another respondent mentioned, "I think one of the biggest things is our staff train our staff to be aware of different things, such as security awareness training on phishing attacks.

RQ 3: Of the technologies and services libraries use, what do IT professionals believe poses the most serious challenge to patron privacy?

The IT professionals in this study pointed out that sometimes software they are using in the libraries could pose serious challenges to patron privacy. For example, they mentioned that **data in patron databases might be breached**; data might **not be encrypted** property; files transmitted over Wi-Fi service for **remote printing** could be seen by non-authorized people. The participants have also been worried about how commonly used **software or services**, such as OverDrive, Open Athens, AWS, Google, SIP2, would handle patrons' private data. How the data was collected, accessed, used, and deleted by library staff could also cause problems in terms of patron privacy protections. Some participating IT

professionals argued their library, or their vendors might **collect more data than they need**. Some libraries allowing multiple staff to use **shared logins** for library system was another concern. Besides data practices, participants also mentioned that their **policies are outdated**. Again, multiple library IT professionals restated that their most serious concern is patrons' lack of knowledge and awareness when they share their personal identifiable information with others or ignore privacy policy when using libraries' services.

RQ 4: From IT professionals' perspectives, what kind of technological changes, if any, should public libraries in general make to better protect patron privacy?

The changes IT professionals suggested included changes about enhancing **library employees' (both IT and non-IT pros') knowledge and skills** on using or configuring hardware and software, offering **patrons' education and training**, and advocating cultural change led by **library administration**. In terms of the changes related to the use or configuration of hardware and software, the IT professionals suggested that libraries should **enhance browser and firewall** to keep data anonymized. In addition, libraries should **enforce data encryption**, and **reduce the data tracked** by IT systems, especially wireless software managed by third-party vendors. For example, one respondent mentioned that:

> I like the fact that in California, we have an opt out in terms of tracking . . . so if you go to a web page, you can opt out, they're not going to track you. But I don't think that's the case across the country. I wish that we could include something like that, with our vendors.

Another participant also emphasized:

> If analytics are so critical to your business and being able to gather data and make data driven decisions and things like that. We just always need to be extremely careful to anonymize any data that we gather so that we're not tying it back to specific person.

Some respondents even suggested libraries should develop their own technologies and software to better protect patron privacy.

For patron education and training, the IT professionals indicated libraries should have a **patron disclosure statement** that helps **patrons be better informed** what information is being collected when using library services, for what purpose, and how the data would be used. They also suggested **both patrons and librarians should be better educated about privacy protections**. One IT professional said:

> The only thing I would say, and this is a whole other subtopic is patron education. There's a lot of things like we can talk about what we can do to protect them as much as we can, but they make choices, so I think patron education as a library focus for privacy concerns is something that's we need to spend more time on.

Similarly, another IT professional also emphasized:

> I think educating the public is an important thing for us to do to explain privacy and how what we do to protect them and why we do what we do.

Last but not least, the library ITs emphasized that besides technological changes, **changes led by library administration** is critical. One participant explained:

> I would say is I don't think we need technological changes, other than the will to do them, but we need our concerted [efforts] by our library administrations to address to talk about and then remediate these issues. For me it's not technological changes, I think it is about cultural change and resources.

Other participants hoped the administrations of their libraries could offer more funding to replace old software that does not follow the best privacy protection practices. For instance, one IT professional strongly expressed that:

> You might not have the money to keep everything up to date. . . . Maybe it doesn't have to be the latest greatest hardware, but I do need to make sure that it's as up to date with its virus protection as it can be. And then it's up to date with the latest version of windows on it until if that hardware can be updated . . . you have to make those decisions.

Participants also recognized the urgency of **ensuring privacy protection policies and practices being approved** by the Board of Trustees of libraries.

We did not observe significant differences in discourse between these focus groups given that the participants were randomly assigned based on their availability. Nevertheless, it is worth highlighting that individuals from smaller libraries expressed a keen interest in innovative solutions to enhance their access to shareable resources and expertise. For example, IT professionals working in smaller libraries proposed that library administration should collaborate with security experts to establish a shared clearinghouse on secure software or services. This collaboration would enable informed decision-making, particularly regarding patron

privacy protections, such as selecting appropriate vendors to work with.

Discussion

Drawing from the insights provided by IT professionals during the focus groups, which highlighted challenges, best practices, and potential improvements related to patron privacy protection, we have formulated a set of recommended strategies for public libraries. These strategies encompass three key aspects: providing adequate training and support to library staff, urging library administration to align privacy protection policies with current practices, and enhancing communications about privacy protections with patrons.

Providing Training and Support to Library Staff to Interact with Technologies

Based on the responses we received from the focus group study, we found many participants recognized the need to configure or update the software and hardware used in public libraries in order to better protect patrons' privacy. However, libraries sometimes lack control over the technologies, and need more training for their staff, both IT-pro and non-IT-pro, to implement these changes. As many small libraries rely on consortiums to provide unified tech supports not customized for their libraries, there is an urgent need for cost-effective and easy-to-use tools or resources that can help these small libraries to better manage their data and technologies for patrons' privacy. This request is consistent with what we learned from previous literature: librarians lack privacy protection training, especially since many were not able to attend training given COVID lockdowns (Wang et al. 2023). A prior study confirms that offering employees education and training can change librarians' viewpoints and raise their awareness of patron privacy protection (Noh 2014). Our findings confirm there is still room for improvement with regard to libraries offering employee training to protect patrons' privacy, particularly from technology aspects.

Urging Library Administration to Align Privacy Protection Policy with Current Practices

As reported in several previous studies, some libraries do not have a privacy policy in place to guide library employees on how to protect patrons' privacy (Wang et al. 2023; Lurd 2021). The findings from this focus group study resonates with the insights learned from the literature and underscores the importance of aligning libraries' existing policies with their current practices. For example, changes to privacy policy and practices are often pending approval by library administration; therefore, their policy is not comprehensive and does not provide details on privacy protection for using new technologies or dealing with the latest privacy-related challenges such as data leakage and law enforcement requests. Concerns that vendors have collected more data than they need should also be addressed. This requires library administration to work closely with the library IT professionals to negotiate with the vendors or set up guidelines regarding data collection and management, to better protect patrons' privacy. From our focus group study, we also found more than half of the participants were not familiar with the American Library Association Library Privacy Checklist. Among those who have heard of or checked the checklist, most mentioned that the checklist "is a good guideline" and it was their "goal" to implement the checklist; however, in reality, they found it was not implementable. There is an urgent need for administrative support to implement the checklist and other best practices aimed at protecting patron privacy.

Enhancing Communications about Privacy Protections with Patrons

One of the major challenges IT professionals reported when implementing best practices of patron privacy protections is patrons lacking the awareness and accurate knowledge toward protecting their own privacy. Although some patrons are aware and concerned about whether their data or information behavior would be seen and tracked by library staff, other patrons, or third- party vendors, many IT professionals indicated **their patrons did not pay attention to privacy or felt inconvenienced when being asked to follow privacy policy**; especially among those who have **lower digital literacy and need library staff's assistance to complete tasks on computers or online**. This has been relatively common in rural and suburban libraries serving **underserved areas** where the IT professionals mentioned that they are working in a small community where library staff and patrons all know each other; thus, patrons do not voice any privacy concerns and feel frustrated when the library staff cannot enter private information for them "given privacy policy." In addition, as some participants confessed, it is not rare that library staff need to **trade patrons' privacy for patrons' convenience per patrons' requests**. They recognized themselves or their colleagues were forced to follow the privacy policy "flexibly" to fulfill patrons' needs; such comprise especially occurs in libraries serving smaller neighborhoods, since the librarians know the patrons standing in front of them and are more likely to bend the rules for such patrons.

To address these concerns, our study participants suggest that public libraries can develop and **offer education or training on privacy protection to library patrons**. For

example, Libraries should provide **publicly available and easy-to-understand education materials** that clearly state what data would be collected from the patrons for which purpose to increase privacy protection awareness and knowledge not only among the staff but also among the patrons. In addition, libraries could **provide technology classes** on privacy to patrons with lower digital literacy, such as **English-as-Second-Language patrons** who often share private information with library staff given that they need librarians' help to fill out online applications. Moreover, libraries should have clearer privacy policies with vulnerable populations, like juveniles, or **offer patrons options to opt in or opt-out** from library services.

In addition to the aforementioned points, as the study participants reiterated, it is vital to underscore the importance of fostering a robust culture of patron privacy protection within public libraries. This responsibility is not exclusive to library administration alone, but extends to every stakeholder involved, including library staff, both IT and not-IT professionals, and library patrons. Protecting patrons' privacy in public libraries is a collective effort that requires aligning practices, polices, funding, resources, and technologies to ensure the effective implementation of privacy protection measures. By recognizing shared responsibility and actively engaging all stakeholders, public libraries can create a safer and more privacy-conscious environment to protect patrons' privacy.

Conclusion

This focus group study was conducted to uncover the unique practices and challenges IT professionals have encountered in their daily work to protect patrons' privacy. To the best of our knowledge, this is the first focus group study that featured insights from IT professionals, who work at the forefront to safeguard patrons' privacy in public libraries. IT professionals found balancing between protecting patrons' privacy and providing customer service has been a serious challenge. They were concerned with the libraries' practices on using patrons' data, expressed the need for more support on configuring software and hardware, and hoped to work with library administrations to improve policy and practices on patron privacy protections. The participants in the focus group study observed discrepancies between their libraries' privacy policy and actual practices when their colleagues do not strictly adhere to the privacy policy, sometimes due to patrons' requests. Our work makes the unique contribution of identifying the concerns and challenges library IT professionals have that need to be addressed to better protect patrons' privacy in public libraries. Public libraries serving underserved communities confront the dual challenge of limited financial and technological resources while striving to balance customer service and privacy protection, especially for patrons with lower digital literacy. This is especially important in the context of rural and small libraries which have several vulnerabilities in their library operations. We also identified the technologies and practices IT professionals use to enhance privacy protection and the technical changes they hope to implement. From these findings, we conclude enhancing patrons' privacy protection communication could mitigate the discrepancies between privacy policy and practices. Library employees sometimes are forced to violate privacy policy when patrons are unaware of or unwilling to follow the best privacy protection practices and request the library employees to trade patrons' privacy for convenience. Patrons' privacy protection education could empower patrons, especially vulnerable populations in underserved communities that highly rely on IT resources in libraries but with lower digital literacy, to better protect their privacy. We also noticed that many library staff requested additional support or guidelines that would help them work with the technologies in public libraries more smoothly. Library administration also plays a critical role in maintaining up-to-date privacy policies and practices. Our findings identify the need for further research to explore what might be missing in the library policy, what kind of training can help patrons better understand privacy protections, and what guidelines or resources should be offered to support libraries to address these challenges on protecting patrons' privacy.

Limitations and Future Directions

Our focus group study was conducted during the COVID-19 pandemic; thus, many participants were working remotely. Although we asked participants to respond based on their regular practices as they had been implemented before and during COVID when they joined the study, some responses might still have been impacted given the fact that people could not meet or work in-person at library sites at the time of the study. In addition, though we clearly stated that all the responses would be anonymized in publications, some participants might still tend to not reveal the failures they observed, or the changes needed to be made to the current privacy policy or practices in their libraries given social desirability bias.

To further replicate and investigate these findings, it would be beneficial if existing privacy protection policies of public libraries were collected and analyzed to better understand best practices as well as policies that would need revisions. This type of study would inform libraries that do not have a policy in place or need help with reviewing and updating their current privacy policy. Additionally, given

that many smaller-sized libraries do not have the resources to address the discrepancies between their privacy protection practices and policy, we are working to develop and distribute guidance and automated tools that can help in a technical aspect, supporting library staff with limited technical background to assess and improve the security and privacy level of their current library systems.

References

Adetayo, Adebowale Jeremy, Pauline Oghenekaro Adeniran, and Arinola oluwatoyin Gbotosho. 2021. "Augmenting Traditional Library Services: Role of Smart Library Technologies and Big Data." *Library Philosophy and Practice* (e-journal): 1–15. https://digitalcommons.unl.edu/libphilprac/6164.

American Library Association. 2006. "Privacy: An Interpretation of the Library Bill of Rights." http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy.

American Library Association. 2015. "Library Privacy Guidelines for Vendors." http://www.ala.org/advocacy/privacy/guidelines/vendors.

American Library Association. 2019. "New Library Bill of Rights Provision Recognizes and Defends Library Users' Privacy." ALA News. www.ala.org/news/press- releases/2019/02/new-library-bill-rights-provision-recognizes-and-defends-library-users.

Asher, Andrew D. 2017. "Risk, Benefits, and User Privacy: Evaluating the Ethics of Library Data." In *Protecting Patron Privacy: A LITA Guide*, edited by Bobbi Newman and Bonnie Tijerina, 43–56. Lanham, MD: Rowman & Littlefield.

Ayre, Lori Bowen. 2017. "Protecting Patron Privacy: Vendors, Libraries, and Patrons Each Have a Role to Play." *Collaborative Librarianship* 9, no. 1. https://digitalcommons.du.edu/collaborativelibrarianship/vol9/iss1/2/.

Bernard, H. Russell, Amber Wutich, and Gery W. Ryan. 2016. "Analyzing Qualitative Data: Systematic Approaches." Thousand Oaks, CA: Sage.

Breeding, Marshall. 2016. "Privacy and Security for Library Systems." *Library Technology Reports* 52, no. 4: 1–35. https://doi.org/10.5860/ltr.52n4.

Bryne, Amelia, and Marijke Visser. 2022. "Keeping Communities Connected: Library Broadband Services During the COVID-19 Pandemic." *ALA Policy Perspectives* 9. https://www.ala.org/advocacy/sites/ala.org.advocacy/files/content/telecom/broadband/Keeping_Communities_Connected_030722.pdf.

Caro, Alex, and Chris Markman. 2016. "Measuring Library Vendor Cyber Security: Seven Easy Questions Every Librarian Can Ask." *Code4Lib Journal*, no. 32. https://journal.code4lib.org/articles/11413.

Corrado, Edward M. 2007. "Privacy and Library 2.0: How Do They Conflict?" https://alair.ala.org/handle/11213/17023.

Corrado, Edward M. 2020. "Libraries and Protecting Patron Privacy." *Technical Services Quarterly* 37, no. 1: 44–54. https://doi.org/10.1080/07317131.2019.1691761.

Cotter, Kelley, and Maureen Diana Sasso. 2016. "Libraries Protecting Privacy on Social Media: Sharing without 'Oversharing.'" *Pennsylvania Libraries: Research & Practice* 4, no. 2: 73–89. https://doi.org/10.5195/palrap.2016.130.

Fortier, Alexandre, and Jacquelyn Burkell. 2015. "Hidden Online Surveillance: What Librarians Should Know to Protect Their Own Privacy and That of Their Patrons." *Information Technology and Libraries* 34, no. 3. https://doi.org/10.6017/ital.v34i3.5495.Harper, Lindsey M., and Shannon M. Oltmann. 2017. "Big Data's Impact on Privacy for Librarians and Information Professionals." *Bulletin of the Association for Information Science and Technology* 43, no. 4: 19–23. https://doi.org/10.1002/bul2.2017.1720430406.

Hennig, Nicole. 2018. *Siri, Alexa, and Other Digital Assistants: The Librarian's Quick Guide*. Englewood, CO: Libraries Unlimited.

Horrigan, John B. 2015. "Libraries at the Crossroads." Pew Research Center: Internet, Science & Tech. September 15. https://www.pewresearch.org/internet/2015/09/15/libraries-at-the-crossroads/.

Institute of Museum and Library Services. 2023. "Access to Public Library Services and Materials During the First Nine Months of the COVID-19 Pandemic." Washington, DC: Institute of Museum and Library Services. https://www.imls.gov/sites/default/files/2023- 05/pls_fy20_research_brief.pdf.

Jaeger, Paul T., and Kenneth R. Fleischmann. 2007. "Public Libraries, Values, Trust, and E-government." *Information Technology & Libraries* 26, no. 4: 34–43. https://doi.org/10.6017/ital.v26i4.3268.

Kritikos, Katie Chamberlain, and Michael Zimmer. 2017. "Privacy Policies and Practices with Cloud-Based Services in Public Libraries: An Exploratory Case of BiblioCommons." *Journal of Intellectual Freedom and Privacy* 2, no. 1: 23–37. https://doi.org/10.5860/jifp.v2i1.6252.

Lambert, April D., Michelle Parker, and Masooda Bashir. 2016. "Library Patron Privacy in Jeopardy an Analysis of the Privacy Policies of Digital Content Vendors." *Proceedings of the Association for Information Science and Technology* 52, no. 1: 1–9. https://doi.org/10.1002/pra2.2015.145052010044.

Loter, Jim. 2016. "Gaining Insights and Protecting Privacy: De-identifying Patron Data at The Seattle Public Library." *The Washington Library Association Journal* 32, no. 1: 11–13. https://wala.memberclicks.net/assets/Alki/alki_mar2016_v32-1-v3.pdf.

Lund, Brady D., and Matt Beckstrom. 2019. "The Integration of Tor into Library Services: An Appeal to the Core Mission and Values of Libraries." *Public Library Quarterly* 40, no. 1: 60–76. https://doi.org/10.1080/01616846.2019.1696078.

Lund, Brady D. 2021. "Public Libraries' Data Privacy Policies: A Content and Cluster Analysis." *The Serials Librarian* 81, no. 1: 99–107. https://doi.org/10.1080/0361526x.2021.1875958.

Lund, Brady D. 2022. "Libraries in a World of Data: How to Move Forward While Protecting Users." In *Technological Advancements in Library Service Innovation*, edited by Lamba, Manika, 182–96. Hershey, PA: IGI Global. https://doi.org/10.4018/978-1-7998-8942- 7.ch011.

Maceli, Monica. 2019. "Librarians' Mental Models and Use of Privacy-Protection Technologies." *Journal of Intellectual Freedom & Privacy* 4, no. 1: 18–32. https://doi.org/10.5860/jifp.v4i1.6907.

Marden, Bill. 2017. "The Path to Creating a New Privacy Policy: NYPL's Story." *Journal of Intellectual Freedom & Privacy* 2, no. 1: 5–7. https://doi.org/10.5860/jifp.v2i1.6295.

McAndrew, Chuck. 2020. "LibraryVPN." *Information Technology and Libraries* 39, no. 2. https://doi.org/10.6017/ital.v39i2.12391.

McCarthy, Justin. 2020. "In U.S., Library Visits Outpaced Trips to Movies in 2019." Gallup. Last modified January 24, 2020. https://news.gallup.com/poll/284009/library-visits-outpaced-trips-movies-2019.aspx.

Morehouse, Shandra, Jessica Vitak, Mega Subramaniam, and Yuting Liao. 2020. "Creating a Library Privacy Policy by Focusing on Patron Interactions." *Sustainable Digital Communities*, 571–78. https://doi.org/10.1007/978-3-030-43687-2_47.

Noh, Younghee. 2014. "Digital Library User Privacy: Changing Librarian Viewpoints through Education." *Library Hi Tech* 32, no. 2: 300–317. https://doi.org/10.1108/lht-08-2013-0103.

Noh, Younghee. 2017. "A Critical Literature Analysis of Library and User Privacy." *International Journal of Knowledge Content Development & Technology* 7, no. 2: 53–83. https://doi.org/10.5865/IJKCT.2017.7.2.053.

Pacific Library Partnership and LDH Consulting Services. 2020. "Data Privacy Best Practices Toolkit for Libraries." https://www.plpinfo.org/wp- content/uploads/2020/10/PLP_Toolkit_Final-Accessibility-Modified.pdf.

Pekala, Shayna. 2017. "Privacy and User Experience in 21st Century Library Discovery." *Information Technology and Libraries* 36, no. 2: 48–58. https://doi.org/10.6017/ital.v36i2.9817.

Pelczar, Marisa, Lisa M. Frehill, Evan Nielsen, Ashley Kaiser, J. Hudson, and T. Wan. 2021. "Characteristics of Public Libraries in the United States: Results from the FY 2019 Public Libraries Survey." Washington, DC: Institute of Museum and Library Services. https://www.imls.gov/sites/default/files/2021-08/fy19-pls-results.pdf.

Pelczar, Marisa, Jake Soffronoff, Jiayi Li, Sara Alhassani, and Sam Mabile. 2023. "Data File Documentation: Public Libraries in the United States Fiscal Year 2021." Washington, DC: Institute of Museum and Library Services. https://www.imls.gov/sites/default/files/2023- 06/2021_pls_data_file_documentation.pdf.

Public Library Association. 2021. "2020 Public Library Technology Survey Summary Report." https://www.ala.org/sites/default/files/pla/content/data/PLA-2020-Technology-Survey-Summary-Report.pdf.

Real, Brian, and R. Norman Rose. 2017. "Rural Libraries in the United States: Recent Strides, Future Possibilities, and Meeting Community Needs." ALA Office for Information Technology Policy. https://www.ala.org/sites/default/files/advocacy/content/pdfs/Rural%20paper%2007-31-2017.pdf.

Sweeney, Miriam, and Emma Davis. 2021. "Alexa, Are You Listening?" *Information Technology and Libraries* 39, no. 4. https://doi.org/10.6017/ital.v39i4.12363.

Tella, Adeyinka. 2019. "Librarians' Perception of Opportunities and Challenges Associated with Big Data in Public Libraries." *Internet Reference Services Quarterly* 24, no. 3–4: 89–113. https://doi.org/10.1080/10875301.2021.1900978.

Thomchick, Richard, and Tonia San Nicolas-Rocca. 2018. "Application Level Security in a Public Library: A Case Study." *Information Technology and Libraries* 37, no. 4: 107–18. https://doi.org/10.6017/ital.v37i4.10405.

Vitak, Jessica, Yuting Liao, Mega Subramaniam, and Priya Kumar. 2018. "'I Knew It Was Too Good to be True': The Challenges Economically Disadvantaged Users Face in Assessing Trustworthiness, Avoiding Scams, and Developing Self-Efficacy Online." *Proceedings of the ACM on Human-Computer Interaction* 2 (CSCW): 1–25. https://dl.acm.org/doi/10.1145/3274445.

Wang, Tian, Chieh-Li Chin, Christopher Benner, Carol M. Hayes, Yang Wang, and Masooda Bashir. 2023. "Patron Privacy Protections in Public Libraries." *The Library Quarterly* 93, no. 3: 294–312. https://doi.org/10.1086/725069.

White, Kristy Lynn, and John Robert White. 2021. "Accepting Free Content during the COVID- 19 Pandemic: An Assessment." *The Serials Librarian* 81, no. 1: 11–19. https://doi.org/10.1080/0361526x.2021.1943106.

Yoose, Becky. 2017. "Balancing Privacy and Strategic Planning Needs: A Case Study in De- Identification of Patron Data." *Journal of Intellectual Freedom and Privacy* 2, no. 1: 15–22. https://doi.org/10.5860/jifp.v2i1.6250.