# Intersectional Thinking about PETs: A Study of Library Privacy

Nora McDonald
George Mason University
Fairfax, VA, USA
nmcdona4@gmu.edu

Rachel Greenstadt
New York University
New York, NY, USA
greenstadt@nyu.edu

Andrea Forte
Drexel University
Philadelphia, PA, USA
aforte@drexel.edu

## ABSTRACT

This qualitative study examines the privacy challenges perceived by librarians who afford access to physical and electronic spaces and are in a unique position of safeguarding the privacy of their patrons. As internet "service providers," librarians represent a bridge between the physical and internet world, and thus offer a unique sight line to the convergence of privacy, identity, and social disadvantage. Drawing on interviews with 16 librarians, we describe how they often interpret or define their own rules when it comes to privacy to protect patrons who face challenges that stem from structures of inequality outside their walls. We adopt the term "intersectional thinking" to describe how librarians reported thinking about privacy solutions, which is focused on identity and threats of structural discrimination (the rules, norms, and other determinants of discrimination embedded in institutions and other societal structures that present barriers to certain groups or individuals), and we examine the role that low/no-tech strategies play in ameliorating these threats. We then discuss how librarians act as "privacy intermediaries" for patrons, the potential analogue for this role for developers of systems, the power of low/no-tech strategies, and implications for design and research of privacy-enhancing technologies (PETs).

## KEYWORDS

anonymity, privacy, libraries, intersectionality

## 1 INTRODUCTION

Libraries in the US have long been staunch defenders of privacy and strategies of anonymity. They traditionally adhere to the principles of privacy and intellectual freedom articulated by the American Library Association (ALA), which supports the use of anonymity as a tenet and tool of intellectual freedom as stated in the Library Bill of Rights, adopted in 1939. But gone are the days when destroying local paper records sufficed to protect patrons' information seeking activities—to keep them anonymous from other patrons and institutions. In today's landscape, library staff who wish to protect their patrons' privacy contend with a complex set of surveillance infrastructures, including those owned by third-party vendors whose resources are accessed by patrons within the library [49, 85], and threats stemming from complex, identity-based vulnerabilities.

Today's libraries provide access to a virtual realm of information that largely resides outside their walls, and even within their walls, it is difficult to regulate or contend with ubiquitous surveillance, whether it be video cameras limiting "anonymous" access to books or vendor databases requiring login for access. Most recently, libraries are being threatened with further limitations on what they can loan which disproportionately affects marginalized[1] users, who depend on digital loans for (surveillance-free) access [49]. Yet as custodians of technology services, librarians have the potential to afford (some) privileges of anonymity. Librarians in a position to provide internet might consider offering anonymous browsing tools and access. The Library Freedom Project, which advocates for and educates librarians on privacy and security and surveillance threats, has introduced Tor relay hosting in public libraries [4, 60].

The challenge librarians face in safeguarding anonymity and privacy is important, given the critical role of libraries in serving the interests of students and educational institutions, as well as the most vulnerable and marginalized public communities. Library literature expresses staunch concern for librarians' ability to protect patrons privacy, for example, on social media (e.g., [59]) and from behavioral data surveillance (e.g., [1] as well as from government institutions (e.g., [55, 56]). Is there something we can learn from the way they think about their role as "service providers" to these communities?

### 1.1 Research question

We set out in this research with the following research question: *How do librarians think about their patrons' privacy and what strategies and technologies do they use to help protect their patrons' privacy?*

### 1.2 "Intersectional Thinking"

While this study was designed to investigate technology practices around privacy and anonymity, we find that many privacy solutions do not leverage technologies at all. Many of the challenges librarians must mediate have to do with managing information privacy in the physical space, including physical and electronic records, as well as computer access, support, and training, and often those challenges have to do with protecting their most vulnerable patrons from structural and oppressive threats. Librarians' efforts in this regard represent a kind of intersectional thinking: taking into account not only patrons' identities as users of the library system, but as individuals with a host of identity characteristics that represent potential vulnerabilities; and not only the system of the library itself, but the multiple potentially oppressive systems that converge to allow for information access in that space. The requirement to think holistically about patrons information environment and risks in relation to their identity often leads to low/no-tech strategies,


*Proceedings on Privacy Enhancing Technologies 2023(2), 480–495*

https://doi.org/10.56553/popets-2023-0064

[1] We define "marginalized" individuals as 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 [76].

like preventing parents from finding about marginalized youth's information interests by keeping library cards separate.

### 1.3 Contribution

We make several contributions with this work.

(1) We describe how librarians we interviewed perceive vulnerable library patrons' identities and the structural threats faced by those patrons, and how these perceptions shape informal, low/no-tech strategies and policies related to the use of privacy infrastructures and data collection.
(2) We show how librarians' concern for the privacy of vulnerable users and the structural disadvantages they face constitutes a kind of intersectional thinking. That thinking leads librarians to protect vulnerable patrons' information in ways attuned to the structural inequalities that exist outside their institutional walls. The primary insight we derive from intersectionality is an appreciation for the ways in which identity-based oppressions potentiate one another, and how these challenges are critically understood in relationship to constructs of power (capitalism, classism, racism, sexism, ableism, etc.) [23].
(3) In light of that, we consider how this intersectional thinking approach offers a starting point for the PETs community to consider how low/no-tech solutions to privacy protection play out on the ground, where technological designs may fall short, and the role of service providers as "privacy intermediaries."

Ultimately, this paper provides a case study of what intersectional thinking looks like in action and, importantly, *the ways that librarians, as privacy intermediaries, use low/no-tech strategies to complement privacy-enhancing technologies and provide the kind of customized privacy protections that they believe are necessary for their patrons to be safe*. We further find that "anonymous" access, as understood by librarians, is viewed as a "privilege" of information-seekers who are vulnerable as a consequence of their goals and interests (such as whistleblowers, journalists, and activists) rather than those who are vulnerable due to features of their identities (e.g., race, income, sexual identity). This research provides insight for the design of sociotechnical privacy mechanisms, and in promoting privacy scholarship that engages with intersectionality—not only as an abstraction, but also as a form of action, of *thinking*. This thinking, we argue, can provide new approaches to designing inclusive PETs that reflect the needs and experiences of vulnerable populations. We argue that PETs researchers should explore how service providers like librarians cope with privacy threats, use intersectional thinking, and support blended technological and non-technological approaches to privacy protections within institutions.

## 2 RELATED LITERATURE

### 2.1 Vulnerable Identities, Privacy, and Libraries

We use the term vulnerable identities to refer to those with one or more facets that put them at increased risk for privacy-related harm. These facets might include minority status, low socio-economic status [62, 78], sexual identity or gender [13, 32, 42, 53, 75, 82], a history of houselessness [58, 96] or domestic abuse [36, 64], undocumented immigration status [44], a criminal record [92] or stigmatized illnesses like HIV [91] as well as the very young [6, 95] and very old [50] and those who are disabled and depend on assistive technologies [46, 93]. In addition to privacy vulnerabilities, we find that librarians also consider the discriminations of low-income, black and brown, immigrant, houseless, and LGBTQ communities by police [5, 31, 81**?** ], the government [30], and online [48, 73, 86].

Vulnerable populations often depend on government services and public libraries, and by virtue of using these public resources, are more susceptible to privacy threats [30]. Merely attempting to access social benefits or pay taxes on insecure or public networks can leave people susceptible to scams and identity threats. The implications of failing to achieve privacy in these realms can result in pervasive, sometimes devastating, vulnerabilities. Through the lens of "class vulnerability," Madden et al. examine how big data, including those gathered through social media, leave these individuals vulnerable to job and education discrimination and predictive policing [61]. For some low-income individuals, experiences with scams and cybersecurity threats are not only financially and psychologically damaging, they can lead to deep distrust of technology and of others [89].

Vitak et al. discovered that for low-income individuals, whose vulnerability can lead to a lack of trust in technology and institutions, librarians represent a vivid exception—a trusted resource on whom the underprivileged may rely heavily for assistance with technology [89]. Many vulnerable individuals have even more reason to be dependent on libraries since stigmatized or marginalized identities often intersect with low socio-economic status [18], leaving them more dependent on free internet access and librarian resources. As a result, these individuals must often submit personal and sensitive identity information when applying for jobs, seeking social services, or filing their taxes through public computers. Some are already uniquely vulnerable to privacy threats; the requirement that they access the internet through public resources increases those vulnerabilities.

*2.1.1 Vulnerable identities and PETs.* Researchers of PETs across disciplines are increasingly considering the ways technologies must take into account the realities and agency of diverse users [65, 94]. Even still, efforts to embrace privacy by design often fail to consider critical alternatives or values, contexts, and structural inequalities [97]. The field of human-computer interaction (HCI), has had to reconcile with its history of focusing on where the construct of the "user" breaks down and the consequences for privacy design [9, 10]. PETs has similarly focused on the way in which the "user" fails to be aware of, or adopt privacy tools (e.g., [2, 88]). By this point, the "user" is arguably a construct resulting from the powerful privacy norms that are particularly exclusionary to the vulnerable [67] and that govern economic systems of surveillance capitalism [98]. Designing for privacy requires consideration of marginalized positions of data citizens and their entanglement in what Couldry and Mejias describe as data extractive systems [24]. Some researchers have pointed out, for instance, the persistence of outdated privacy constructs (e.g., "confidentiality") and the fact that privacy technologies do not occur in a vacuum but rather are constitutive, meaning that identities and historical contexts matter [45]. In a critique of PETs,

Gürses argues that tools that support anonymity and confidentially should not be abandoned, but reconsidered in light of a system of surveillance in which they currently offer little protection (a false sense of security) and individual burden [45]. Moreover, Gürses argue that fights for privacy must be waged at the database (or service provider) level [45]. Although Gürses wrote over a decade ago, these assertions hold up.

*While clearly lack of protection against surveillance infrastructures has implications for policy and regulation and systems design, we also argue that this has implications for how we conceive of PETs—not just as technologies or tools in the traditional sense, but also as socially and politically motivated practice.* We find that librarians rely on human-computer collaboration to deliver the kind of privacy their patrons require to keep them safe, and which are not (fully) available just by using the technology they have.

## 2.2 Privacy vs Anonymity: PETs and the Library

Privacy affords individuals freedom from involuntary disclosure by conferring on them the right to shield personal information in a variety of contexts. Early PETs scholarship classified privacy into four categories: "'freedom from intrusion', 'negotiating the public/private divide', 'identity management' and 'surveillance"' [77]. The power to control identity management and surveillance (what this paper is most interested in) resides with the individual and with powerful norms—which in a panoptic society [34] rest on compliance, apathy, and powerlessness (or resignation [28]) and also may be much more impactful for those with less privilege. Consequently, privacy is typically described as both an individual mechanism for revealing and concealing aspects of the self and as a contextual norm of information flows (e.g., who has access to what information) [66].

Anonymity, when considered as a way of facilitating privacy, is typically something individuals seek, not simply to protect identity information but also to withhold it. Even this withholding can be selective—for instance, when someone conceals their IP address from a service provider but reveals their real name to a community of users. Anonymity requires both social and technical forethought in its execution, which means that someone should consider not just what information is revealed but also by whom it can be seen and used. While it allows one to achieve greater privacy, anonymity is, in fact, an instrument, not an absolute end. Most people don't achieve, or intend to achieve, full anonymity. According to Gary Marx, full anonymity would require subverting seven dimensions of identity knowledge including: legal name, location, traceable pseudonyms, untraceable pseudonyms, behavior patterns, social categorizations, and personal characteristics [63]. Regardless of what level of concealment is necessary, PETs systems that provide anonymity (e.g., VPNs, Tor) and pseudonymity are sometimes challenging to use. Although speaking of PGP and other privacy software, Phillips argues that this is because they are "operationally complex," socially opaque, require effort and bestow rewards that are abstract [77]. More recently, research suggests that non-experts struggle to use anonymous browsing tools like Tor in ways that don't compromise anonymity [37].

Library scholars have, for some time now, noted the potentially diminishing role of libraries in this conversation about privacy protections and the need to acknowledge evolving privacy threats [51] and to advocate for their patrons [57, 59]. For example, there are growing concerns about the connection of mobile devices to library networks [71]. Providing anonymous access doesn't come without risks (and, as noted, burdens that are insurmountable and possibly futile [45]) and libraries must weigh the benefits of providing patrons with surveillance-free access against the potential risks [39].

# 3 CONCEPTUAL FRAMING OF THIS RESEARCH: INTERSECTIONALITY

We frame our findings through the lens of intersectionality. Intersectional theory expands traditional feminist theories to account for simultaneous identities that together may magnify individuals' susceptibility to systems of discrimination. Intersectional theory allows us to consider the "marginal" or "invisible" user whose context (e.g., roles, information, relationships) demands an alternate narrative, distinguished from the "typical" user or personas invoked in design processes [79].

We draw primarily on Crenshaw's concepts as well as Collins and Bilge but note that intersectionality has a long history grown out of the black feminist movement [20–22, 47], and more recently has shifted thinking about research in computing [35, 54, 80, 87].

Intersectionality is "on its way to becoming a critical social theory" and the diversity of its use has been a boon to its development towards social change [22]. A core tenet of intersectionality is the critical importance of thinking about power in relationship to multiple, interconnected social coordinates and vulnerabilities. One foundational insight of intersectionality is that identities and/or "conditions of social and political life" are "not shaped by any one factor" [23], that they build on one another, and that to understand the connections requires an examination of identities in relation to power over time [25].

Crenshaw introduced the concept of structural intersectionality to show how policies overlook the multidimensionality of experience [26]. She uses the example of a battered women's shelter where policies assume a certain narrative about newcomers which effectively ignore other dimensions of experience (structural discrimination in US laws, poverty, conditions of immigration, etc.) and systematically exclude people from entering based on a narrow definition of threat. Her account exposes the vast chasm that can exist between what we imagine people's obstacles to be and the reality on the ground. We will demonstrate how librarians are similarly concerned about the importance safeguarding multiple dimensions of identity and experience. For example, librarians might perceive that a patron who is a minor in the care of adult guardians, and also a member of the LGBTQ community, could find themselves subject to surveillance. Librarians describe privacy protections needed to protect patrons against oppressive power relationships and structural disadvantages that entangle them.

What we aim to do by introducing the term "intersectional thinking" is to suspend our conceptions of normative privacy as a framework for analysis and consider instead what people actually do when they think intersectionally about the management of privacy

in their personal lives. Intersectionality, envisioned by Crenshaw was always about combinations. But, again, while she most notably (and famously) focused on black women in her seminal essay, she also looked at immigrant women of color who survive abuse and the complex layers of discrimination (e.g., lack of access to information, culture and language barriers, discriminatory US laws) to account for the ways in which they are prevented from getting help [26]. In recent discussions Crenshaw and collaborators further examined how intersectionality moves and grows in new domains to address new constituencies [19].

Collins and Bilge (among others) articulate how intersectionality grapples with dynamic complexities of race, class, gender, and systems of normative and discriminatory power in the context of social and political conditions [23]. The interdependence of coalitions to social inequality, power, culture, etc. allows Collins and Bilge to explore how intersectionality's critical framework can be applied to topics ranging from black Brazilian feminism to football players in the World Cup. Intersectionality is not about finding a race+class (or other) equation that operates with analytical precision; it's about taking a critical lens to interlocking oppressions operating in an environment that is loaded with complexities (so they sometimes operate in lock-step and sometimes in less coherent ways) and, yes, our own (in-group) biases about how things operate. In this way, Bilge and Collins usefully highlight the way intersectionality is about the dynamics of identity and power in a given context.

In her book, *Intersectionality as Critical Social Theory*, Collins asks, "What exactly is an intersectional way of thinking" [22]. She goes on to say that, a critical key to this question is found in reflections by Crenshaw (who "coined" the term) about its use as a metaphor. According to Collins, Crenshaw's metaphor was "recognizable to many people because it invoked the tangible, spatial relations of everyday life." The librarians we interviewed are thinking about the intersectional dimensions of their patrons' lives. They see their patrons, they enter records, and they decide who they share information with on a case-by-case basis. These information practices do inform their guidance and decision-making around technology use. But what we found most interesting and useful for HCI and PETs researchers was the holistic and integrative way in which they consider patrons' privacy.

As we analyzed our data, we found intersectionality to be an important analytical lens for this inquiry because not only do librarians seem to have a perspective on relationships that link identity, lived experience and power, they are in a clear position to mediate them. They also, critically, understand the importance of how information can enact oppression. We follow Crenshaw's lead in using intersectionality to promote equity by considering its use as a mechanism for privacy-related thinking, policy work and change [27]. Although intersectionality emerges from an intellectual tradition, it is, perhaps just as critically, an intuitive framework for librarians conditioned on their experience. In this paper, we focus attention on real-life privacy protective practices and actions that we find are predicated on intersectionality as a way of thinking.

# 4 RESEARCH DESIGN

Because we wanted to gather data about how librarians think about privacy, and how they understand the threats faced by their patrons, we adopted a phenomenological approach to research that focuses on understanding their first-hand experiences. As described in detail below, we conducted interviews as our data collection method and used thematic analysis to analyze the data.

## 4.1 Interview Participants

*4.1.1 Recruitment.* To recruit participants, we sent email messages to library staff from local institutions in the spring of 2019 to invite them to participate in a 30-90-minute interview. We started out by recruiting from low-and high-resource institutions to get a balanced perspective. We also, at times, used "snowball sampling" [74], which resulted in recommendations of participants at that same institution. We generally followed up with people who were said to offer another perspective or a have more experience.

As the analysis progressed, we used a purposeful, theoretical approach to sampling in order to address emerging questions and account for gaps in the library contexts represented by our participants [40]. After developing a sense of privacy concerns with low-resourced public libraries in economically challenged neighborhoods, we sought out participants from well-resourced library systems.

Participants were given $25 in cash or an Amazon gift card as a thank-you.

*4.1.2 Sample.* Ultimately, we spoke with 16 librarians from 11 different institutions on the East Coast of the United States: 11 participants from 7 public libraries; 4 participants from 3 university libraries, and 1 participant from a government library.

The librarians with whom we spoke represent a wide range of demographics, from medium to large institutions serving students and diverse communities. We recruited from low and high resource institutions to get a balanced perspective. While our sample includes some participants who belong to a network of librarians promoting privacy issues, we purposely sought out five individuals from outside that network, notably finding no discernible differences in their sensitivity to privacy issues. We suspect, however, that there is more variability than what we were in a position to observe with respect to institution type and demographics, as well as, relatedly, funding and resources (e.g., who provides for internet resources).

Since all but 2 of our 16 participants identified themselves as librarians (those exceptions include one library staff member and one pursuing a master's degree in Library and Information Science), we refer to the participants as librarians in reporting our results.

*4.1.3 Ethical considerations.* Our study was approved by our Institutional Review Board and we applied additional ethical considerations in our approach to preserving confidentiality for our participants. Because interview participants spoke about security issues and sometimes asked to make sure they were kept anonymous, we ensured confidentiality for participants and the organizations they represented. We took pains to ensure that our records and transcripts were as anonymous as possible. All demographic information, and to the extent possible, institution names, were collected on paper/off record.

Out of consideration for potential harms, we omitted details about patrons that could be recognized by them. We also do not use participant identifiers when quoting them in this paper.

The practices highlighted by library staff reflect, in some instances, their own thinking about what is right to do, as well as longstanding practices that may or may not be part of formal policy. In one instance, a librarian reflects that their practice is how they do it but not necessarily how their co-workers, who are less tolerant or more conservative in their views, might do things.

## 4.2 Data Collection and Analysis

*4.2.1 Interview protocol.* In each interview, we first asked participants to describe the services they offer, how people make use of these resources, and what information is required. We asked librarians about how they support patrons' privacy needs and about concerns patrons might have about their privacy, but never asked about patrons' identities. (See Appendix A for the interview protocol). In their responses, librarians characterized the kinds of privacy they provide based on the identities and life experiences of their patrons—based on race, history of abuse, sexual or gender identity, and housing status. Borrowing from the privacy and security literature's use of threat models [53], the second part of the interview focused on perceptions of threats by asking participants to describe activities that cause problems for their libraries and their responses to these activities. Demographic data were collected at the end of the protocol, once the recording was off.

We interviewed participants using technologies they were comfortable with, such as phone and Skype. Participants were asked if they consented to recording before each interview. They were told that they could stop at any time. Interviews were audio-recorded and transcribed with participant permission.

*4.2.2 Epistemology and analysis.* We take a subjective, phenomenological approach [83] to understanding perceptions of threats and their influence on privacy decisions and policy.

One researcher led analysis, and interpretations were developed through regular discussion with coauthors. We open-coded initial interviews and then flagged initial themes through coding and memo-writing. We then applied these themes to later interviews, memoing the entire time. The methodological basis for this analysis is the constant comparative method [40] in which data are iteratively collected and coded to identify concepts and in which analysis is heavily directed by the primary researcher. We ultimately used intersectionality to interpret our findings, such that our analysis did not produce new theory, rather it maps to concepts introduced by intersectionality, such as structural intersectionality introduced in the previous section. Our findings reflect librarians views as expressed in the interviews.

We followed best practices for inductive, interpretive thematic analysis per McDonald et al.'s guide to "Reliability and Inter-rater Reliability in Qualitative Research" [70]. In such research, the goal is to develop a robust and integrated explanation of a phenomenon grounded in qualitative accounts using iterative rounds of analysis. Initial coding of interview data revealed that librarians readily pointed to certain identity characteristics of patrons as requiring more careful and unconventional or nuanced consideration in terms of privacy (e.g., those relating to LGBTQ, houseless, low-income minorities, etc). They also revealed tensions that arose in terms of their patron's values and institutional and associated structural challenges. These observations became central features of our analysis and informed the development of our central findings related to intersectional thinking. Although we call out when we are referring to "some" or "a few" or "one" participant, our method yielded an integrated explanation of librarians' practices, not a quantitative analysis.

# 5 FINDINGS

Privacy is closely associated by librarians with the needs, vulnerabilities, and structural challenges of certain socio-economically disadvantaged groups who are also LGBTQ, underprivileged youth, minorities, immigrants, and older adults, all of whom are thought by librarians to warrant special privacy safeguards to protect them from abuse or harassment and encourage participation in library services.

Librarians worry a great deal about producing as little information as possible about patrons to lower barriers in several key ways: not requiring a residence (e.g., for houseless individuals); giving youth (particularly minorities and LGBTQ) penalty-free access without a parent guarantor; giving LGBTQ freedom to explore sexual identity unhindered or not be "retraumatized" at check out if their ID does not match their gender; protecting undocumented and minorities from security, local, state, and national authorities; and avoiding "policing" minority patrons.

Throughout our findings, we focus on librarians' understanding of patrons' concerns (the nature of which is intersectional) rather than the specific struggles or intersectionality of patrons' identities. People who are members of the above-named groups are perceived by librarians to require additional support in their pursuit of access because they may have particular need for safe identity exploration (e.g., LBGTQ) or may require access to information without putting themselves at legal risk or within risk of surveillance (e.g., undocumented immigrants, minorities).

We found that librarians often say they offer privacy by concealing certain identity information in a deliberate way that ensures, for instance, that patrons leave no trace or are not identifiable by authorities; this almost always require the use of low/no-tech strategies such as not handing over records. Librarians say they are responsible for maintaining the privacy of patrons' physical (e.g., books, printed papers) and electronic activities (e.g., web browsing) and records (e.g., library cards, sign-in). This puts librarians in a unique position to view privacy in a holistic way.

Notably, most librarians are aware of technology installed on their computers to erase patrons data. While some comment that they often have to remind patrons that software is installed on computers to reboot and erase personal data (e.g., Deep Freeze), others, in libraries where information is not erased immediately, say they have to remind patrons to not to leave their personal information and files exposed. But most importantly, librarians do not see these technologies as privacy panacea, not only because their patrons are confused about how they work (or that they work at all) but also that they perceive there are other privacy threats to patrons pursuit of information and use of their services—threats

which they feel obligated (and more or less equipped) to offer and do so using low/no-tech, human-computer strategies.

In our findings, we first describe librarians use of privacy technology and their threat models, which mostly compels them to take up low/no-tech solutions. We then define anonymity's limited role. We originally set out to understand how librarians protect patrons' anonymity, particularly by incorporating anonymity-preserving tools into their privacy protocols, but we found that anonymity tools themselves have only limited utility within the library context. A customized and selective approach to anonymity that varies from person to person and considers the diverse forms of oppression they may be subject to (or "intersectional thinking") seems to be librarians favored approach to protect their patrons from harm.

Next, we describe what an "intersectional way of thinking" [22] is and how it influences the type of privacy librarians provide. In many instances, we find that librarians understand providing privacy as a way to restore agency or protect people from discrimination and they do this by considering their identity and the oppressions they may experience outside their walls. Then, we discuss how librarians safeguard vulnerable patronage with intersectional privacy practice, which is related to both protecting personal information (e.g., from authorities, parents, teachers, etc.) and lowering barriers (e.g., fine forgiveness, requiring less identity information, creating an environment where people don't feel policed). These low/no-tech strategies[2] results in informal privacy protection policies. We follow this with an in depth discussion of the types of vulnerable users librarians worry about most and the specific privacy strategies they use. Finally, we discuss the ways in which institutional structures and community norm violations can put stress on intersectional thinking.

## 5.1 Privacy Technology and Threat Models

While librarians were aware of that there is software installed on library computers that erases patrons data, either after each use or at the end of the day, they were often not familiar with what it does, or not convinced that it was effective. But as we will discuss in subsequent sections, librarians primarily described concerns about threats from outside the library. When they described protecting individuals from those threats, it was often not readily associated with technologies; for example, not wanting to identify an individual who caused a disturbance by keeping any record of their behavior. Notably, librarians described taking care to enforce rules that protect the most vulnerable among their patrons while not harming others. They described a desire for libraries to be a "safe space" free from fear of surveillance, technological or otherwise. As we will describe in subsequent sections, librarians' threat models incorporate structural oppression and complex issues of power and discrimination.

[2]We use the term "low/no-tech strategies" to refer to a range of improvised steps taken by librarians to safeguard patrons' privacy without resorting to automated digital tools. We elaborate on these strategies in our findings, particularly in Section 5.4 and 5.5. Some examples of these low/no-tech strategies include personally withholding or concealing records (or not creating them); keeping separate accounts or records and library cards for parents and children (or not requiring them at all); printing out items on their own (librarian's) account, etc.

## 5.2 Anonymity's Limited Role in the Stacks and Online

We included questions about anonymity in our interview protocol because it is historically a central theme in librarians' role as privacy stewards. Anonymity, either in the stacks or on the internet, was seen as benefiting primarily activists, whistle blowers, and journalists—an often more privileged group of people whose interests might be perceived as having potential to cause harm to themselves or others, not individuals whose very identity produces vulnerabilities and whose information-seeking in the service of existential needs may put them at risk of unwelcome attention. Despite the assumption that activity, more than status, creates the need for anonymity, participants universally feel anonymity is important for all users in order to access library resources, even if their library doesn't necessarily provide it. This was an area where many typically felt unable to effect change or didn't want to expend "capital," even while reporting all the ways in which they daily author and enact their own policy with regard to vulnerable patrons.

*5.2.1 Anonymous access through Tor.* We asked librarians about Tor, thinking that the library might either be hosting entry and relay nodes or have the Tor browser installed on computers. Neither was the case. Tor is an anonymity network that allows users to browse the web without revealing their IP address. All that a service provider, or anyone looking, can see is the fact that Tor IP are being used. Those who want to support the network can operate what are called entry and relay nodes that are used by the network to connect to online services and thus hide Tor users' original IP. This is a project that has been taken up by some libraries [4] but none that we spoke with.

Because most librarians we interviewed have some familiarity with services like Tor, or even personal use experience, we examined participants views on Tor to frame their thinking about anonymity and privacy. Librarians did consider that vulnerable populations, including those who have experienced being houseless and immigrants, might benefit from using a Tor browser. Yet, even while the librarians we interviewed believe having a Tor browser would be useful in their libraries, many doubt it would ever pass IT hurdles due to negative "dark web" connotations or technology deficits in their library network.

## 5.3 Intersectional Thinking

Librarians offer a form of selective and deeply thoughtful anonymity, or what we refer to as "intersectional thinking" about privacy practice. Building on Crenshaw's structural intersectionality, we define intersectional thinking as the deliberate (and almost entirely low/no-tech) concealment of certain identifying information for vulnerable populations in ways that are adapted to the structures of inequalities, mainly existing outside institutional walls. It is, perhaps, an inverted conception of contextual integrity—the idea that privacy relates to contextual norms or collective expectations of information flow [72]. Indeed, past research indicates that for marginalized individuals, in particular, privacy might be better achieved for those who employ much less technical strategies or abstinence [78, 90]. Librarians are worried about the relationships their patrons have

with police, parents, and schools which might make them vulnerable, leading librarians to conceal identity or adopt certain practices, not all of which deal with privacy in obvious ways (e.g., ignoring library card usage to avoid penalties). This is a departure from normative analytical frameworks that tend to look at the world through the lens of shared values with little sensitivity to structural inequalities.

Intersectional thinking was a useful lens because librarians take into account different kinds of threat vectors, sometimes digital or electronic and sometimes physical, but do not necessarily aim to make distinctions. Their approach is more holistic. Adopting their perspective, we similarly discuss the privacy protections librarians offer largely without partitioning the digital/electronic from the physical, or from the underlying structures of oppression.

Librarians often display sensitivity to the needs of vulnerable populations based on their closer sight line, but as a general rule, have little in the way of formal policy to support or guide them in extending protection to those populations. As a result, librarians find themselves bending or interpreting rules to accomplish their objectives, as we will discuss more in the next section. By contrast, specific inquiries about "anonymity" or Tor, although believed to be important to offer, often elicit abstract notions of privacy and threats that are perceived to largely affect privileged users (e.g., whistleblowers) who have concerns based on the information they seek.

The remainder of our findings focus on how librarians employ intersectional thinking to provide a type of unique and customized privacy for their vulnerable patrons. These approaches often employ low/no-tech strategies, such as not requiring or handing over information about patrons.

## 5.4 Intersectional Thinking Practice, Threats, and Safeguards

The challenges faced by the vulnerable patrons about whom librarians are most concerned (discussed in the next section) often come from without (e.g., police, government, parents, more opaque threats having to do with safety) and sometimes, though less often, from within (e.g., their own internet habits, other library staff who lack sensitivity or training as well as the systems they use to house resources).

Virtually all of these challenges are addressed by concealing identity knowledge in some form, which sometimes means bending rules or creating them where there are none. In order to provide this kind of privacy, library staff exhibit what is sometimes a profound awareness of, and sensitivity to, the experiences and structural inequalities that make this identity knowledge more harmful. In effect, they are thinking about how power behaves in relationship to identity information.

Many librarians we interviewed perceive the structures and bureaucracies that surround them to be insufficiently sensitive to the needs of the patrons they serve, and when formulating privacy precepts, are often reacting to structural racism (e.g., policing and housing situations that thwart access).

*5.4.1 Low/no-Tech strategies related to intersectional thinking.* Librarians are also concerned about barriers to library resource access among vulnerable groups, often leading them to provide more deliberate low/no-tech privacy, depending on the circumstances, for instance: requiring less identifying information when houseless or LGBTQ patrons sign up for a card; letting identification requirements slide for underprivileged children and parents who want to benefit from penalty forgiveness or just take out more books; not calling or giving information to police about infractions or medical emergencies, in or outside the library; not giving information to parents or schools about what children are reading or when they are in the library to provide intellectual freedom and access to self-discovery and to avoid abusive or hostile situations at home; moving security away from the entrance so that patrons who come from neighborhoods where they are heavily policed are not intimidated; and waiving late fees for patrons whose means are thought to be limited. We elaborate on these improvised low/no-tech strategies in the next section.

Some of these strategies are part of a broader set of accommodations that do not necessarily relate to privacy per se, but which nevertheless align with a view that vulnerable communities should be protected. These accommodations are explicitly connected with perceived structural discrimination, and with situations in which librarians often find themselves having no policy or even an informal playbook to support their decisions.

## 5.5 Vulnerable Populations that Librarians Worry about as Part of Intersectional Thinking & Improvised Low/No-tech Strategies Used

When the librarians we interviewed talk about privacy, it is often with a vulnerable identity in mind, of a sort that relates to structures of inequality. When asked about patron privacy, it was common for librarians to bring up the experiences of patrons with certain identities (e.g., minority youth, LGBTQ, older adults, houseless, immigrants, moms with financial burdens).

To be clear, librarians did not have access to information about patrons' race, self-identified sexual or gender identity, abuse, or housing status. Librarians nevertheless felt they were able to observe or learn about some of these characteristics through interaction with, and getting to know patrons, and this knowledge made them more vigilant about providing tailored privacy to protect those that they suspect might be at risk for privacy violations—e.g., by authorities, parents, spouses, etc.

Out of worry for the privacy of vulnerable patrons in particular, public libraries require as little identifying information as possible to ensure that parents, governments, and authorities are unable to get access to that information. Librarians say that the focus of their concern are minority populations—namely people of color and LGBTQ:

> "Yeah, I'm focused mostly on minority populations. Whether it's people of color or LGBTQ…Those are the main people that I want to make sure that their information is not breached, not disseminated without their permission…"

This librarian goes on to point out that they worry about a range of issues for these individuals from someone finding out about what

they read to them not feeling welcome in their library because of their identity, which because of their relationship with police and authorities might leave them feeling unsafe:

> "If you're LGBTQ, you don't want people to know that you're reading it necessarily. Or, if you're a person of color you may always feel like you're in a position of vulnerability. We want to make you feel welcome at our library, so we want them to know that we're doing everything in our power to make sure that they feel safe and secure in our facilities."

Along those lines, some participants point out that they don't confront parents using their children's cards because they don't want to "police" or "hamper" adults in any way that might make them feel unwelcome out of similar concerns for societal oppressions.

> "You know, it's not going to kill anybody to come in here and use the internet. ... So I don't need to check to see if you're using your child's card."

Because Librarians are hesitant to "police" use of cards, out of concern for privacy and structural issues of oppression outside their walls, they say they have adopted a way of dealing with people not wanting to use cards or using other people's cards on a "case-by-case" basis:

> "[I]t ends up being very case-by-case … I mean, you can argue for or against that. But just even really simple things, like people wanting to check out books without having their library card. So, then you have to decide whether to give them access to the account without that sort of proof. And in most cases, you do that."

Librarians we spoke with say that, additionally, they may also opt to reduce information requirements to secure a library card in the service of protecting access for the underprivileged, who face structural barriers. For instance, this might apply to patrons who may not have the required information (such as a permanent residence) or who may be challenged to afford fees. Librarians' enforcement of privacy protections may sometimes speak more to their intersectional thinking about a range of policies that could limit patrons' access than a specific commitment to privacy; they are worried about any barriers to providing a safe space for information and discovery.

To that end, residency information can be a barrier for both citizen and non-citizens, given the kinds of identification that the library systems may formally require. Several librarians note that people who are houseless can get access to the library using their shelter address, while another librarian laments that people without state issued ID (mostly houseless and non-citizens) can't use the library. As one librarian remarks, these are the patrons who need it the most and so they bend the rules:

> "In general, I'll take an EBT card which is not officially sanctioned, but I mean, come on. Especially when you're dealing with patrons who are experiencing homelessness. ...they're exactly the people who need our resources the most."

Librarians' enforcement of privacy protections may sometimes be coincidental and speak more to their intersectional approach to policy than commitment to privacy. But for them it's part of the same way of thinking and that is important. As this librarians points out, the people who need library resources the most are those that do not have identification. At the same time, it's clear that privacy and lower barriers are inextricably intertwined.

*5.5.1 Special case of minors.* Children are a special case of vulnerable individuals, in part because librarians say they worry about how young age intersects with so many other experiences of adversity. These may include socio-economic disadvantage and an associated lack of after-school options, an abusive home environment, and LGBTQ status. Sensitivity to the needs of disadvantaged or stigmatized minors and concern about potential lack of access explain why libraries offer penalty-free cards and allow for access without a guardian (i.e., to give them privacy from guardians). Some offer special programs that allow students to access books with just a lunch number, which "give[s] the students who go to school a quick way of picking out books without having to have a library card." That is, they understand how different domains of power might place burdens on children.

One way in which libraries extend protection to vulnerable minors is by not requiring parental guardianship on cards. As one librarian noted, this latitude gives youth the freedom to explore sexual orientation without judgement:

> "And, I'm thinking mostly like, LGBTQ people, in that range and things kind of in that vein. Where they may not come from a supportive household, they may be struggling with their sexual orientation but they know they can't go to their parents for it. So, I'd really want them to come to our library and be able to get the information they need to make the decisions that are best for them. So, that's one reason why I don't want the guarantors."

The same librarian stresses that self-checkouts allow LGBTQ teens to explore/access the stacks freely and stresses trying to maintain all aspects of patron's privacy, "the physical and the digital":

> "I also like to stress that we have self-checkouts. So, if you are uncomfortable with the books that you're checking out, whether you're a teen looking at something about eating disorders, you're a member of the LGBT community, you don't want really people to see that you're reading this … I like to balance the physical and the digital privacy to make sure the patrons know that we're trying to respect it in every avenue possible."

Preventing parents from finding out what their children are reading or not giving any information to parents or schools when they call looking for a child is seen as as a way of protecting them from family situations that could be detrimental to self-discovery or even abuse. Understanding of how one could be linked to the other (sexual orientation, culture, abuse) and who is a threat is again why this intersectional lens is so helpful. Also critical is the idea of creating a "safe space" outside of power structures for young adults. The result is policies already mentioned, ranging from offering

minors their own card, ensuring privacy of what they take out when parents do sign off on cards, and ensuring that parents and school to not have access to their attendance while at the library. Several librarians spoke about not letting parents or schools know about the whereabouts of minors in their library:

> "[If] a parent or a teacher called to see if the teen was there, we generally don't give the phone...because it could be a vulnerable situation and we don't want to put anyone in an uncomfortable position or a dangerous position … I mean, I think in extreme cases I would worry that ... if a teen lived in a home where they don't feel safe, and they're using the library because it feels like a safe space, then that would be a break in trust and maybe by keeping this a safe space, we can help them out a little bit. So ... if someone knows that their teen is at the library, maybe it's not a great home situation, that might put the teen in danger."

According to this same librarian, ensuring the library is a "safe space" means not giving out information.

Another librarian worries about kids who pick up books being abused by their parents and so wants to make sure they provide privacy from parents about what their children are reading:

> "I would say a child maybe who picked up a book on dealing with abuse. I wouldn't want to give that information to their parents who might be an abuser."

Then there is the issue of protecting people's gender identity. While some states have officially adopted policies with no gender identification requirement, a few librarians from other states without such policies point out that not all their colleagues are equally sympathetic to the issue, with the result that an individual could be continually misgendered when using the library.

> "Me, as a library worker, could just go in and change it. Depends on how the staff member wants to respond, which is a whole separate issue. I have seen people who identify as a gender that is not the one that is on their ID with a different name. And I've seen staff members refuse to change the name and refuse to change the gender marker for the purpose of them saying it is otherwise a misrepresentation of the person, and it won't match their ID. Because if you lose your library card, you can use your state ID to access your account or get a new library card."

Librarians said they were not necessarily even sure why the gender requirement was removed in their institution (if it had been) but noted that, regardless, it was not information they needed.

## 5.6 Intersectional Thinking about Privacy Practice Tradeoffs and Tensions

The kind of privacy protections offered by librarians involve tradeoffs that often take into account intersectional realities and, by consequence, often place librarians in opposition to institutional power structures and harmful norms.

Because they are aware of the history of violence and surveillance by police, library staff are quick to defend and extend protections for patrons to ensure they are not unfairly targeted or traumatized in a space the library staff strives to make welcoming. As a result, librarians might try to block the police or not cooperate with them. Their protections also extend to creating buffers against family members who seek information and to supporting patrons who cannot afford to pay. All these decisions involve tradeoffs—for instance, by creating a more permissive environment in which quiet and order are harder to maintain. This section describes those tradeoffs, as they are critical to understanding the "librarian as service provider" model.

The threats reported by librarians that necessitate consideration of tradeoffs are those that disrupt the library environment, such as noise, fighting, eating, sexual deviance, videotaping, pranks, watching porn (which can sometimes upset other nearby patrons), or harassing library staff through chat. Some of these infractions can have serious repercussions for violators since libraries may have policies, either written or informal, that temporarily ban patrons from accessing library resources.

For librarians, intersectional thinking involves lowering barriers—similar perhaps to an open source service provider model[33]—and interpreting and bending policy in ways that take into account challenges faced by users that often originate outside the library. For instance, the librarian who imagines that aggressive physical behaviors are meant as a spectacle to counter physical threats by others and resists intervening unless absolutely necessary. Or the librarian whose boss believes that security guards will be perceived as threatening and thus situates them so that they are not visible to create a more inviting environment. By creating privacy from seeming authority figures, from whom patrons fear discrimination, or worse, librarians hoped to mitigate any chilling effects.

Librarians felt that providing privacy was a means of restoring agency or protecting their patrons from the outside world in which they may not feel as free to seek out information but that can sometimes conflict with the autonomy and sense of privacy of those within their walls.

For example, in the discussion about security guards, the librarian whose boss limits their presence said that while security is there to enforce noise policies, that presence can seem intrusive and intimidating to patrons who experience harassment by police in their neighborhoods. This librarian recognizes that guards can, both help create a safe and welcoming space, while simultaneously create an intimidating and unsafe space for people who were subject to surveillance and over-policing:

> "So, that's something that, I think we've been struggling with, because some students want quiet space. Some students want to socialize, and it's hard to, like, maintain both of those atmospheres and have everyone be happy. And, like I mentioned earlier, like, my chief librarian was, you know, aware that the security guard can intimidate young students, particularly, people who have, like who come from communities where they're getting harassed by police. So, she didn't want the, like, security guard to be front

> and center, because it might make the library seem unwelcoming."

In this case, intersectional thinking about the oppressions (profiling by police, discrimination, etc.) faced by complex identities prompt librarians to lower barriers for those seeking to participate.

In general, librarians are very reluctant to get police involved given the relationship between vulnerable populations and law enforcement and describe situations in which they have not given records to police:

> "I don't want to be introducing police into [this] space ... when you're dealing with institutional racism ... you know, you definitely don't want to bring the police in."

For this librarian, recognition of institutional racism and its impact on patrons' ability to seek out information in a safe space means not allowing the police into the library.

Police are perceived to be a hostile force and even if confronted with physical violence among patrons, librarians try to avoid involving them to resolve disputes. Again, intersectional awareness of police as a source of surveillance for their most vulnerable patrons leads librarians to provide alternative strategies like resolving disputes themselves, or even, in some cases, blocking people from the library without involving authorities. In every case, they avoid turning over records to police—even if the library might maintain them. That said, librarians sometimes reported that although keeping the police away was consistent with their values, they had no training for these types of situations:

> "My favorite is one time they came in and the guy had a Blue Lives Matter shirt on and it's just like, 'Jesus man, know your audience.' How do you deescalate that situation? And again, right, going back to the library school thing, no one ever used the word deescalate once in all of my library school classes. But I would say about half of my day is spent just deescalating."

Despite what this librarian says about police being insensitive, they also pointed out that police generally know to stay away.

Tensions can also arise when trying to protect patrons from privacy violations from school or family. Libraries offer penalty-free (i.e., no late fees) access to minors without parent guardians or guarantors (e.g., their school) to lower barriers, particularly for minority and low-income youth. However, well-intended accommodations can create challenges. Open access to minors means that there is no way to contact responsible adults for issues ranging from needed supervision to disciplinary action to nurturance and care. Librarians understand that collecting (and using) information about parents or guardians may conflict with their professional obligation to maximize access for minors, but they also worry that without some recourse to parents, they cannot fulfill other obligations, both to young patrons and to the community. For example, when minors act out and librarians are not able to contact parents because they don't have email or phone numbers, the result can be banning from the library. In this case, the cost of well-intended privacy protections can be high.

> "… I've never worked for a library before that did require a minor's card to have a responsible parent or caregiver's contact information linked to it. If we ever have an issue arise with kids, if I am not able to access their account and get that phone number or email, it can be really hard to contact somebody that can be able to help me … I look up the address and there's no information linking to a parent or guardian. So that can be a little frustrating."

Another example of tensions is expressed by an employee of a university that services a lot of minority and English as a Second Language (ESL) students. This librarian worries about some of the vendors' connections with US Immigration and Customs Enforcement (ICE) and, in related conversation, about how easy it might be for Department of Homeland Security (DHS) to get access to the records of immigrant students, adding that it's hard for them to say with regard to intellectual freedom whether JSTOR[3] is any safer than Google. This librarian worries about the analytics stored by universities and companies like JSTOR, particularly if they were to get in the hands of DHS.

> "Like, it's hard for me to even say that, library resources, particularly, like, electronic resources, are like, 'safer to use,' than Google in terms of, like, data collection and stuff like that. Because, they collect just as much. Some of those companies collect just as much information about, like, your behavior as Google does. ... Like, if [DHS] were to get student records about who is undocumented, that would be an easy way for DHS to harass, and like, intimidate, and potentially, like, harm the students. So, that's something I think about."

This librarian describes how they had recently researched connections between the services they use to grant patrons access to online databases and organizations like ICE. This notion of the risk posed by surveillance to vulnerable patrons is something that librarians are both cognizant of, and also worried about.

## 6 DISCUSSION

To lower barriers for vulnerable communities, librarians seek less information about patrons and/or attempt to tightly manage and tailor information flows in extemporaneous ways in order to offset vulnerabilities experienced by individuals at elevated risk relative to the community overall. Insofar as this strategy seeks to customize privacy protection rather than honor group norms and averages, it runs counter to an approach that prioritizes a contextual integrity framework [72]. The privacy protections that librarians aim to provide are attentive to the idea that social division and heterogeneity can make a "one-size-fits-all" policy suboptimal for the individual, even if suitably efficient for the community as a whole. This may explain why so few librarians acknowledge having a formal privacy policy per se, even while advancing shared beliefs that appear to reflect privacy sensitivities—for instance, their self-designated youth advocacy role, which sometimes puts them at odds with parents

[3] A digital library, JSTOR is short for Journal Storage.

or other authority figures in an attempt to protect the privacy of minors and dependents.

## 6.1 Intersectional Thinking vs Anonymity

We went into this study believing that anonymity technologies might play a larger role, but when librarians reflect on anonymity, or use of tools like Tor, they connect it with a privileged group of users who wish to avoid scrutiny of their interests and activism. Discussion of anonymity focused on privileged information seekers—that is, those whose identities don't leave them vulnerable but whose interests and queries may (e.g., someone seeking information on making a bomb). In other words, intersectional thinking did not appear connected to anonymity seeking as a form of privacy protection. Librarians accepted the idea that economic models and power structures limit their ability to provide anonymity either on the web or even sometimes in the stacks or on printers. Shoshana Zuboff has characterized the ways in which privacy is defined under capitalism as surveillance capitalism [98]. Scholars have argued that this pervasive vulnerability to monitoring necessitates explicit regulation rather than trusting shared social norms or collective notions of privacy to protect us [38, 45].

## 6.2 Intersectional Strategies Based on Different Types of Vulnerabilities

For the librarians we interviewed, different types of vulnerability map to different types of privacy strategies—and almost always those strategies are low or non-technical. For example, librarians who were concerned about communities being over-policed and having hostile relationships with law enforcement were more lenient about disruptive or seemingly threatening behaviors. They were also wary of enforcing behavioral rules to avoid escalating situations to the point where authorities might become involved or some patrons might be alienated, even while acknowledging the dilemma that other patrons might be troubled by lack of order. Others with the same worries might situate security personnel in the back of the library, or maintain strict policies about anonymity when police are called.

Librarians' perspective-taking on behalf of patrons also extended to children and family relationships. Other examples include, withholding permission from parents to share cards, or failing to disclose the presence of children when schools or parents call looking for them. In each case, librarians are acting around, or outside of contextual norms in order to create a secure environment for children in accordance with their own judgment of what might constitute safety or security.

## 6.3 Intersectional Thinking: Broad Implications for Design and Research

Because many of the librarians we spoke with consider reality on the ground (structures of discrimination that define and shape the experiences of those most vulnerable), we found intersectional thinking (or intersectional privacy practice) to be a useful framework for interpreting our results. Librarians are intersectional in their perspective-taking, imagining the structural inequalities that exist outside their walls, which causes them to interpret and bend policies or rules (if they exist) to support privacy for library users in a way that online communities may not.

The idea that library staff are intersectional in their thinking relates to their ability to imagine the unique challenges faced by patrons because of their identities and their relationship to structures of oppression. An example of this would be consideration for the immigrant patrons who are from neighborhoods that are highly surveilled. In this case, nationality, socio-economic, and structural inequality associated with targeted policing leads library staff to conclude that having guards front and center could be threatening—that is, guards who are there to surveil and police, and thus strip patrons of their privacy. This is a kind of intersectional perspective-taking applied to privacy. Another illustrative finding comes from an insight by a librarian that patrons sometimes need to seem threatening to protect themselves, a pattern that creates discomfort or psychological vulnerability for other patrons. Library staff are, in effect, left with the challenge of trying to accommodate the need for safety by extending permissions for certain non-normative behavior while still creating an environment that feels safe for all.

This intersectional mindset allows librarians to be "privacy intermediaries"[4] in interesting and surprising ways and this maps to their role as being first and foremost gatekeepers to information and knowledge resources. Importantly, librarians tend to profile their patrons according to these vulnerable identities and connect them with informal policies around requiring less information or erasing data in pursuit of knowledge. Thus, there is something potentially to be learned from librarians' role as privacy intermediary. Focusing on vulnerable identities (and provisions of intersectional privacy practice) is important not only because it focuses our attention on the most susceptible and on those who stand to lose the most, but also because our normative frameworks are not equipped to render them.

Echoing research of scholars in this field, librarians do sometimes lament that patrons have misconceptions about managing their privacy settings [43] and about their visibility [3], and that privacy concerns are a weak predictor of actual behavior [7, 8, 52]. Yet research, particularly on youth, suggests a different interpretation, presenting users as knowledgeable about the risks associated with online media and surveillance but helpless to do anything about it—precisely because they are all too familiar with the consequences of offline surveillance [62]. Pitcan et al. find that marginalized social and economic positions amplify risks online and contribute to avoidance of social media and self-censorship [78]. Thus while privacy paradox phenomena is increasingly being debunked or replaced with resignation [28, 84], marginalized individuals have not had the luxury of resignation. Rather, they might have, as literature suggests, to learn to avoid certain technology or behaviors altogether.

One implication is that privacy intermediaries may be essential for those who feel helpless, and for whom the consequences are dramatically different, particularly in environments where these attitudes are informed by the realities of offline surveillance. In the

[4]We use the term "privacy intermediary" to describe librarians' improvised role as intersectional privacy stewards and mediators between their patrons and various institutional and personal forces that threaten them. But we believe this role could be extended to other service providers. We elaborate on this role in Section 6.5.

next sections we talk about the implications of privacy intermediaries for the larger privacy technology and computing community.

## 6.4 Use of Low/No-Tech Strategies

For vulnerable individuals, the experience of privacy threat (in the form of surveillance risk) is more pronounced—both in frequency and magnitude. That puts them at elevated risk of digital privacy invasion and leads them (or librarians) to be more attuned to privacy risks and incursions, and, as we demonstrate, this leads to different kinds of tactics. Marginalized communities (and those that support them, like the librarians we studied) can thus be instructive in their use of low or non-technical solutions and abstinence.

Librarians spoke of the threats that affected their communities. And these threats led them to advocate for low/no-tech approaches. While in many cases, the threats themselves seemed low/no-tech (e.g., parents calling looking for their kids or police looking for names of patrons), it's possible that librarians may have offered non-tech strategies in the face of more technical attacks. For instance, if librarians feared their patrons were being tracked on their phones by parents, they might have advocated not using a phone *at* the library (or *going to* it). Of course, librarians did not bring this up and/or seemed only to be aware of parents attempting to surveil their children by calling up the library and through their library card. But while librarians did not offer more technical strategies, they never lamented not having them.

For the moment, there is little technical solution for surveillance by police or others—for being tracked or profiled with a phone or apps by geolocation or internet searches (e.g., [14]) which librarians do worry about, but can do little to affect. Of course, anonymous browsing may become a more frequently considered solution for librarians seeking to shield patrons from surveillance and future research might (re)explore how it is being used.

While marginalized populations (and, in this case, librarians) have been addressing threats to their digital privacy (e.g., predictive policing, surveillance, and exploitation) enabled through government policies (or lack thereof) with low/no-tech solutions and abstinence (non-technical), privacy scholars have been focused on technical solutions, overlooking the way in which these technical solutions are particularly untenable for marginalized and vulnerable individuals.

## 6.5 Privacy Intermediaries: Service Provider Models and Implications for PETs

For librarians and libraries, our findings raise some interesting design issues around questions of "privacy" from whom and privacy for what? Librarians view providing privacy is a means of gaining back agency or protecting people from discrimination. Critical black scholars have argued that surveillance technologies perform oppression [11, 16]. As privacy intermediaries, librarians seem well aware of the risks and are also willing to consider how these infrastructures are part of the library apparatus, while also acknowledging that they represent a problem to be solved. **What this may mean for PET designs is the empowerment of librarians to play a service provider role, with explicit latitude to modify or adapt the rules and negotiate access on patron's own terms and thus lower barriers and provide safe histories of participation** [33]. Examples might include, not requiring unique identifiers (librarians are often managing the risk of forgoing them today) and negotiating normative violations inside the library based on a situationally sensitive approach that takes account of norm-based threats outside their walls. Importantly, tensions do arise from librarians taking these stances, which often put them in opposition to powerful policies and institutions. This needs to be taken into account when considering this model. That said, we believe this model could extend to other contexts where service providers provide access to privacy vulnerable groups as defined in McDonald and Forte [68].

*Librarians' role as privacy intermediaries* means that they think about information flows on behalf of their patrons and beyond their immediate sphere. They navigate the world beyond their walls and imagine the realities of individuals in a context not shared. Librarians serve as the intermediary between their realm and the institutions and actors outside. For instance, third-party services offer the ability for library users to seek information beyond the library walls, but produce vulnerabilities. Third-parties may not consider that they are organizations from which library users need protection. Librarians do. Librarians imagine that they, as well as relatives and loved ones (not just governments and police) are potential threats to their patrons and this makes them more nimble and creative when it comes to privacy—at times standing in for what is not available to enhance privacy. **Researchers and designers of PETs can follow the example of librarians by including ourselves as potential adversaries and considering vulnerabilities in our threat models, our personas, and part of every design phase. We should consider the vulnerabilities of users as resulting from communities and structural inequalities, and not just other users.**

In their role as privacy intermediary, librarians leverage intersectional thinking to take into account a multiplicity of experiences and a matrix of structural oppression[5], and construct privacy enhancing configurations of which PETs scholars should take note. In reflecting on "privacy as practice," Gürses argues that PETs should help users to understand "what data exists about them ... how it travels and how it is used, and to comprehend ways of improving privacy practices in the future" [45]. We argue that this burden is already being shouldered by librarians as service providers who are in a position to negotiate terms on behalf of the user—often within a gray area of institutional guidelines—and that their interpretation of information flows includes consideration of structural inequalities. **We wonder if this model could be expanded to PET designs for internet collectives and other social institutions whose sight line into local challenges and structural inequality puts them in a similar position to advocate on the side of "users." This is a new concept of a service provider role—breaking with the traditional paradigms that, even in**

[5]Patricia Collins puts forth the notion of the "matrix of domination" or intersecting vectors of power to describe the way in which different groups, with different encounters with discipline and power and privilege, have only partial perspectives [22]. The four tenants of Collins' matrix of domination are domains of power in each realm: interpersonal (how people's actions shape power relations), disciplinary (which rules apply, to whom, and when; e.g., bureaucratic organizations perform routine surveillance for the sake of efficiency), hegemonic or cultural (conditions under which power takes hold) and structural (how powerful institutions are organized; e.g., laws, policies, etc.)

**the best scenarios, are limiting for marginalized users [69]. In a certain sense, this conception removes the question (or burden) of user adoption in that it doesn't consider the user as consumer of PET tools (a consumer responsible for privacy control) but rather a participant whose rights and values are continually seen and heard by those in a position to advocate on behalf of them. Perhaps, then, what we are talking about is not privacy infrastructure or technologies, exactly, but a system of privacy in opposition to the exploitative and extractive systems in place.**

Assuming broad applicability of these implications, a summary of implications for PETs:

- Consider the role of service provider advocates as privacy intermediaries that provide latitude to adapt privacy rules, particularly for marginalized users. Privacy intermediaries may be essential for those who feel helpless, particularly in environments where helplessness is predicated on the realities of offline surveillance.
- Consider the designer's role as potential adversary as librarians do and the implications for tradeoffs. Librarians have heightened awareness that they may end up acting (or being compelled to act) against the interests of their users, especially more marginalized users. This is a thought process that guides the type of privacy they offer—e.g., not creating records.
- Incorporate structural inequality and marginalized individuals into persona and scenario building. Consider that marginalized individuals are increasingly the proverbial "canaries" for the risks of surveillance technologies. Could reflective toolkits be an essential part of PET designs?
- Consider systems of privacy protections that include ad hoc low/no-tech strategies rather than focusing on technology solutions.
- Expand PETs to work with internet collectives and institutions with the outcome not being tools but mechanisms for participation of marginalized individuals and their advocates, whose rights and values they represent. That is, habitually situate PETs within a system of intersectional privacy practice that resists exploitative and extractive systems.

### 6.6 Future Work

These findings have inspired us to consider more deeply the concept of service provider surrogacy, where librarians (and potentially other advocates) would be in a position to negotiate privacy on their patrons' behalf. This means patrons yield some control but also gain more freedom from outside surveillance. This idea creates intimacy between local partners, while blocking outside surveillance actors and adversaries. It might even borrow from the concept of obfuscation [17] where one librarian stands in for many patrons and thus, makes activities harder to trace. Such an approach is also not without risk and requires an activist orientation.

## 7 CONCLUSIONS AND LIMITATIONS

Perhaps because librarians occupy a space in which they serve their users in both the physical and digital realm, they have insight into the social realities experienced by their patrons and the way personal identities and circumstances shape motives and needs. This perspective gives librarians a unique sight line into the risks their users face, and it fosters an empathy that helps them to apply and design privacy strategies that protect them. Intersectionality is being used in this paper as an analytical lens that we are applying to librarians as service providers, who are situated at the critical intersection of identities and power. This frame has given us the opportunity to critically inspect how we think about design and study of privacy, particularly for vulnerable groups.

Our research was conducted before the COVID pandemic, so we did not capture the turmoil or stress on library systems caused by lockdowns and increased use of virtual tools. Most libraries are open once again, so the pre-pandemic interviews are perhaps more relevant than if we had conducted them when libraries were closed.

We also see our results as increasingly relevant given recent events, including the "shadow pandemic" (increased violence against women during COVID) [29] and the overturn of Roe v Wade both of which exacerbate challenges faced by many marginalized groups [12, 15, 29, 41]. While we can only speculate, we see our findings as potentially relevant to understanding the "safe spaces" that the library may provide for these vulnerable individuals and the kind of critical consideration of privacy threats that is characterized by intersectional thinking.

While we sampled from a variety of demographic locations, we would have liked to sample a wider range of rural areas as well, where politics and community norms, as they relate to social issues, may be quite different. In one of our interviews, we were told that politics plays a big role in shaping policy. This raises the question of how consistently local politics and community values influence the exercise of privacy protections in libraries, and to what degree library science training is a socialization process that fosters broad-based sensitivity to the unique role of libraries in their protection of patron privacy. Future work could explore these issues using quantitative methods to survey libraries nationally.

### 7.1 Positionality

As white women and university professors, we are aware that our lens is influenced by privilege and a lack of full understanding into the challenges of the patrons who librarians discussed.

## ACKNOWLEDGMENTS

This work was supported in part by the National Science Foundation grant CNS-1703736.

## REFERENCES

[1] 2021. Resolution on the Misuse of Behavioral Data Surveillance in Libraries. https://www.ala.org/advocacy/intfreedom/datasurveillanceresolution
[2] Ruba Abu-Salma, M. Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. 2017. Obstacles to the Adoption of Secure Communication Tools. In *2017 IEEE Symposium on Security and Privacy (SP)*. 137–153. https://doi.org/10.1109/SP.2017.65 ISSN: 2375-1207.
[3] Alessandro Acquisti and Ralph Gross. 2006. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In *PETS*. 36–58. https://link.springer.com/chapter/10.1007/11957454_3
[4] Julia Angwin. 2015. First Library to Support Tor Anonymous Internet Browsing Effort Stops After DHS Email. https://www.propublica.org/article/library-support-anonymous-internet-browsing-effort-stops-after-dhs-email
[5] Julia Angwin, Jeff Larson, Surya Mattu, and Lauren Kirchner. 2016. Machine bias. *Pro Publica* (2016).

[6] Bushra Anjum. 2018. An Interview with Pamela Wisniewski: Making the Online World Safer for Our Youth. *Ubiquity* 2018, December (Dec. 2018), 2:1–2:6. https://doi.org/10.1145/3301323

[7] Susan B. Barnes. 2006. A privacy paradox: Social networking in the United States. *First Monday* 11, 9 (Sept. 2006). http://firstmonday.org/ojs/index.php/fm/article/view/1394

[8] Susanne Barth and Menno D. T. de Jong. 2017. The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics* 34, 7 (Nov. 2017), 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

[9] Eric Baumer and Andrea Forte. 2017. Undoing the Privacy Paradox with Data Styles. In *2017 Networked Privacy Workshop at CSCW*. Portland, Oregon, USA.

[10] Eric P. S. Baumer and Jed R. Brubaker. 2017. Post-userism. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. Association for Computing Machinery, Denver, Colorado, USA, 6291–6303. https://doi.org/10.1145/3025453.3025740

[11] Ruha Benjamin. 2019. *Race After Technology: Abolitionist Tools for the New Jim Code* (1 edition ed.). Polity, Medford, MA.

[12] Michele W. Berger. 2022. Overturning Roe disproportionately burdens marginalized groups. *Penn Today* (2022). https://penntoday.upenn.edu/news/overturning-Roe-abortion-bans-disproportionately-burden-traditionally-marginalized-groups

[13] Lindsay Blackwell, Jean Hardy, Tawfiq Ammari, Tiffany Veinot, Cliff Lampe, and Sarita Schoenebeck. 2016. LGBT Parents and Social Media: Advocacy, Privacy, and Disclosure During Shifting Social Movements. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 610–622. https://doi.org/10.1145/2858036.2858342

[14] Sarah Brayne. 2020. Enter the Dragnet. *Logic Magazine* 12 (2020). https://logicmag.io/commons/enter-the-dragnet/

[15] Khiara M. Bridges. 2017. *The Poverty of Privacy Rights* (1 edition ed.). Stanford Law Books, Stanford, California.

[16] Simone Browne. 2015. *Dark Matters: On the Surveillance of Blackness*. Duke University Press Books, Durham.

[17] Finn Brunton and Helen Nissenbaum. 2016. *Obfuscation: A User's Guide for Privacy and Protest* (reprint edition ed.). The MIT Press, Cambrigde, Massachusetts London.

[18] Human Rights Campaign. 2019. Being African American & LGBTQ: An Introduction. https://www.hrc.org/resources/being-african-american-lgbtq-an-introduction/

[19] Devon W Carbado, Kimberlé Williams Crenshaw, Vickie M Mays, and Barbara Tomlinson. 2013. Intersectionality: Mapping the movements of a theory. *Du Bois review: social science research on race* 10, 2 (2013), 303–312. Publisher: Cambridge University Press.

[20] The Combahee River Collective. 2017. *The Combahee River Collective Statement*.

[21] Patricia Hill Collins. 2015. Intersectionality's Definitional Dilemmas. *Annual Review of Sociology* 41, 1 (2015), 1–20. https://doi.org/10.1146/annurev-soc-073014-112142

[22] Patricia Hill Collins. 2019. *Intersectionality as Critical Social Theory*. Duke University Press Books, Durham.

[23] Patricia Hill Collins and Sirma Bilge. 2016. *Intersectionality* (1 edition ed.). Polity, Cambridge, UK ; Malden, MA.

[24] Nick Couldry and Ulises A. Mejias. 2019. *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford University Press.

[25] Kimberle Crenshaw. 1989. Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine. *University of Chicago Legal Forum* 1989, 1 (1989).

[26] Kimberle Crenshaw. 1991. Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Color. *Stanford Law Review* 43, 6 (1991), 1241–1299. http://www.jstor.org/stable/1229039

[27] Kimberle Crenshaw. 2017. Kimberlé Crenshaw on Intersectionality, More than Two Decades Later, Columbia Law School. https://www.law.columbia.edu/news/archive/kimberle-crenshaw-intersectionality-more-two-decades-later

[28] Nora A Draper and Joseph Turow. 2019. The corporate cultivation of digital resignation. *New Media & Society* 21, 8 (Aug. 2019), 1824–1839. https://doi.org/10.1177/1461444819833331 Publisher: SAGE Publications.

[29] Ramya Emandi, Jessamyn Encarnacion, Papa Seck, and Rea Jean Tabaco. 2021. *Measuring the Shadow Pandemic: Violence against women during COVID-19*. Technical Report. UN Women. https://www.unwomen.org/en/news/in-focus/in-focus-gender-equality-in-covid-19-response/violence-against-women-during-covid-19

[30] Virginia Eubanks. 2018. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Press, New York, NY.

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

[32] Andrea Forte, Nazanin Andalibi, and Rachel Greenstadt. 2017. Privacy, Anonymity and Perceived Risk in Open Collaboration: A Study of Tor Users and Wikipedians. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*.

[33] Andrea Forte and Cliff Lampe. 2013. Defining, Understanding and Supporting Open Collaboration: Lessons from the Literature. *American Behavioral Scientist* 57, 5 (2013), 535–547. https://doi.org/10.1177/0002764212469362

[34] Michel Foucault. 1976. *The History of Sexuality, Vol. 1: An Introduction* (reissue edition ed.). Vintage, New York.

[35] Sarah Fox, Amanda Menking, Stephanie Steinhardt, Anna Lauren Hoffmann, and Shaowen Bardzell. 2017. Imagining Intersectional Futures: Feminist Approaches in CSCW. In *Companion of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW '17 Companion)*. ACM, New York, NY, USA, 387–393. https://doi.org/10.1145/3022198.3022665

[36] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI'18)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3173574.3174241

[37] Kevin Gallagher, Sameer Patil, and Nasir Memon. 2017. New Me: Understanding Expert and Non-Expert Perceptions and Usage of the Tor Anonymity Network. 385–398. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/gallagher

[38] Oscar H. Gandy. 2017. Surveillance and the Formation of Public Policy. In *Surveillance & Society Biennial Conference*. https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/award2016/6112

[39] Martin L. Garnar. 2012. For the Sake of One Child: Privacy, Anonymity, and Confidentiality in Libraries. *Journal of Information Ethics; Jefferson* 21, 1 (2012), 12–20. https://doi.org/10.3172/JIE.21.1.12

[40] Barney Glaser and Anselm Strauss. 1967. *The Discovery of Grounded Theory: strategies for qualitative research*. Transaction Publishers, New Brunswick.

[41] Michele Goodwin. 2020. *Policing the Womb: Invisible Women and the Criminalization of Motherhood*. Cambridge University Press, Cambridge, United Kingdom ; New York, NY.

[42] Mary L. Gray. 2009. *Out in the Country: Youth, Media, and Queer Visibility in Rural America* (1st edition ed.). NYU Press, New York.

[43] Ralph Gross and Alessandro Acquisti. 2005. Information Revelation and Privacy in Online Social Networks. In *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society (WPES '05)*. ACM, New York, NY, USA, 71–80. https://doi.org/10.1145/1102199.1102214

[44] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H. Mhaidli, Kentaro Toyama, and Florian Schaub. 2018. Keeping a Low Profile?: Technology, Risk and Privacy Among Undocumented Immigrants. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, 114:1–114:15. https://doi.org/10.1145/3173574.3173688

[45] Seda Gürses. 2010. PETs and their users: a critical review of the potentials and limitations of the privacy as confidentiality paradigm. *Identity in the Information Society* 3, 3 (Dec. 2010), 539–563. https://doi.org/10.1007/s12394-010-0073-8

[46] Foad Hamidi, Kellie Poneres, Aaron Massey, and Amy Hurst. 2018. Who Should Have Access to my Pointing Data? Privacy Tradeoffs of Adaptive Assistive Technologies. In *Proceedings of the 20th International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS '18)*. Association for Computing Machinery, Galway, Ireland, 203–216. https://doi.org/10.1145/3234695.3239331

[47] Ange-Marie Hancock. 2016. *Intersectionality: An Intellectual History* (1 edition ed.). Oxford University Press, New York, NY.

[48] Karen Hao. 2019. Facebook's ad-serving algorithm discriminates by gender and race. *MIT Technology Review* (2019). https://www.technologyreview.com/2019/04/05/1175/facebook-algorithm-discriminates-ai-bias/

[49] Lia Holland and Jorydn Paul-Slater. 2022. A major publishing lawsuit would cement surveillance into the future of libraries. *Fast Company* (July 2022). https://www.fastcompany.com/90773185/a-major-publishing-lawsuit-would-cement-surveillance-into-the-future-of-libraries

[50] Dominik Hornung, Claudia Müller, Irina Shklovski, Timo Jakobi, and Volker Wulf. 2017. Navigating Relationships and Boundaries: Concerns Around ICT-uptake for Elderly People. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 7057–7069. https://doi.org/10.1145/3025453.3025859 event-place: Denver, Colorado, USA.

[51] Scott D. Johnston. 2000. Rethinking Privacy in the Public Library. *International Information & Library Review* 32, 3-4 (Sept. 2000), 509–517. https://doi.org/10.1080/10572317.2000.10762534

[52] Adam N. Joinson, Ulf-Dietrich Reips, Tom Buchanan, and Carina B. Paine Schofield. 2010. Privacy, Trust, and Self-Disclosure Online. *Human–Computer Interaction* 25, 1 (Feb. 2010), 1–24. https://doi.org/10.1080/07370020903586662

[53] Vanessa Kitzie. 2019. "That looks like me or something i can do": Affordances and constraints in the online identity work of US LGBTQ+ millennials. *Journal of the Association for Information Science and Technology* 0, 0 (2019). https://doi.org/10.1002/asi.24217

[54] Neha Kumar and Naveena Karusala. 2019. Intersectional Computing. *Interactions* 26, 2 (Feb. 2019), 50–54. http://doi.acm.org/10.1145/3305360

[55] Sarah Lamdan. 2019. Librarianship at the Crossroads of ICE Surveillance – In the Library with the Lead Pipe. *In the Library with the Lead Pipe* (2019).

https://www.inthelibrarywiththeleadpipe.org/2019/ice-surveillance/
[56] Sarah Shik Lamdan. 2013. Why library cards offer more privacy rights than proof of citizenship: Librarian ethics and Freedom of Information Act requestor policies. *Government Information Quarterly* 30, 2 (April 2013), 131–140. https://doi.org/10.1016/j.giq.2012.12.005
[57] Sarah Shik Lamdan. 2015. Social Media Privacy: A Rallying Cry to Librarians. *The Library Quarterly: Information, Community, Policy* 85, 3 (2015), 261–277. https://doi.org/10.1086/681610 Publisher: The University of Chicago Press.
[58] Christopher A. Le Dantec and W. Keith Edwards. 2008. The view from the trenches: organization, power, and technology at two nonprofit homeless outreach centers. ACM Press, 589. https://doi.org/10.1145/1460563.1460656
[59] Monica Maceli. 2019. Librarians' Mental Models and Use of Privacy-Protection Technologies. *Journal of Intellectual Freedom & Privacy* 4, 1 (June 2019), 18–32. https://doi.org/10.5860/jifp.v4i1.6907 Number: 1.
[60] Alison Macrina. 2015. The Library Freedom Project: Bringing privacy and anonymity to libraries | The Tor Blog. https://blog.torproject.org/guest-post-library-freedom-project-bringing-privacy-and-anonymity-libraries
[61] Mary Madden, Michele Gilman, Karen Levy, and Alice Marwick. 2017. Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans. *Washington University Law Review* 95, 1 (Jan. 2017), 053–125. https://openscholarship.wustl.edu/law_lawreview/vol95/iss1/6
[62] Alice Marwick, Claire Fontaine, and danah boyd. 2017. "Nobody Sees It, Nobody Gets Mad": Social Media, Privacy, and Personal Responsibility Among Low-SES Youth. *Social Media + Society* 3, 2 (April 2017). https://doi.org/10.1177/2056305117710455
[63] Gary T Marx. 1999. What's in a Name? Some Reflections on the Sociology of Anonymity. *The Information Society* 15, 2 (1999), 99–112.
[64] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F. Churchill, and Sunny Consolvo. 2017. Stories from Survivors: Privacy & Security Practices when Coping with Intimate Partner Abuse. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 2189–2201. https://doi.org/10.1145/3025453.3025875 event-place: Denver, Colorado, USA.
[65] Nora McDonald, Karla Badillo-Urquiola, Morgan G. Ames, Nicola Dell, Elizabeth Keneski, Manya Sleeper, and Pamela J. Wisniewski. 2020. Privacy and Power: Acknowledging the Importance of Privacy Research and Design for Vulnerable Populations. In *CHI'20 Extended Abstracts*.
[66] Nora McDonald and Andrea Forte. 2020. The Politics of Privacy Theories: Moving from Norms to Vulnerabilities. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376167
[67] Nora McDonald and Andrea Forte. 2021. Powerful Privacy Norms in Social Network Discourse. *PACM on Human-Computer Interaction. CSCW* 5, 2 (2021).
[68] Nora McDonald and Andrea Forte. 2022. Privacy and Vulnerable Populations. In *Modern Socio-Technical Perspectives on Privacy*, Bart P. Knijnenburg, Xinru Page, Pamela Wisniewski, Heather Richter Lipford, Nicholas Proferes, and Jennifer Romano (Eds.). Springer International Publishing, Cham, 337–363. https://doi.org/10.1007/978-3-030-82786-1_15
[69] Nora McDonald, Benjamin Mako Hill, Rachel Greenstadt, and Andrea Forte. 2019. Privacy, Anonymity, and Perceived Risk in Open Collaboration: A Study of Service Providers. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI '19)*. ACM, New York, NY, USA. https://doi.org/10.1145/3290605.3300901
[70] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and Inter-rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (Nov. 2019), 72:1–72:23. https://doi.org/10.1145/3359174
[71] J. B. Choice Napp. 2018. User privacy: a practical guide for librarians. *Middletown* 55, 12 (Aug. 2018), 1448. http://search.proquest.com/docview/2077526184/citation/7A46A58CB7134C72PQ/1
[72] Helen Nissenbaum. 2009. *Privacy in context: technology, policy, and the integrity of social life.* Stanford Law Books, Stanford, Calif. OCLC: 436310287.
[73] Safiya Umoja Noble. 2018. *Algorithms of Oppression: How Search Engines Reinforce Racism* (1 edition ed.). NYU Press, New York.
[74] Charlie Parker, Sam Scott, and Alistair Geddes. 2020. Snowball Sampling. In *SAGE Research Methods Foundations* (paul atkinson, sara delamont, alexandru cernat, joseph w. sakshaug & richard a. williams ed.). SAGE Publications Ltd, 1 Oliver's Yard, 55 City Road, London EC1Y 1SP United Kingdom. https://doi.org/10.4135/9781526421036831710
[75] Susan Patricia Patterson, Shona Hilton, Paul Flowers, and Lisa M. McDaid. 2019. What are the barriers and challenges faced by adolescents when searching for sexual health information on the internet? Implications for policy and practice from a qualitative study. *Sexually Transmitted Infections* 95, 6 (Sept. 2019), 462–467. https://doi.org/10.1136/sextrans-2018-053710 Publisher: BMJ Publishing Group Ltd Section: Digital communications and sexual health.
[76] Katy E. Pearce, Amy Gonzales, and Brooke Foucault Welles. 2020. Introduction: Marginality and Social Media. *Social Media + Society* 6, 3 (July 2020), 2056305120930413. https://doi.org/10.1177/2056305120930413 Publisher: SAGE Publications Ltd.
[77] David J. Phillips. 2004. Privacy policy and PETs: The influence of policy regimes on the development and social implications of privacy enhancing technologies. *New Media & Society* 6, 6 (Dec. 2004), 691–706. https://doi.org/10.1177/1461448042042523 Publisher: SAGE Publications.
[78] Mikaela Pitcan, Alice E. Marwick, and danah boyd. 2018. Performing a Vanilla Self: Respectability Politics, Social Class, and the Digital World. *Journal of Computer-Mediated Communication* 23, 3 (May 2018), 163–179. https://doi.org/10.1093/jcmc/zmy008
[79] John Pruitt and Jonathan Grudin. 2003. Personas: Practice and Theory. In *Proceedings of the 2003 Conference on Designing for User Experiences (DUX '03)*. ACM, New York, NY, USA, 1–15. https://doi.org/10.1145/997078.997089
[80] Yolanda A. Rankin and Jakita O. Thomas. 2019. Straighten Up and Fly Right: Rethinking Intersectionality in HCI Research. *Interactions* 26, 6 (Oct. 2019), 64–68. http://doi.acm.org/10.1145/3363033
[81] Rashida Richardson, Jason Schultz, and Kate Crawford. 2019. Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice. *New York University Law Review Online* (2019). https://www.nyulawreview.org/online-features/dirty-data-bad-predictions-how-civil-rights-violations-impact-police-data-predictive-policing-systems-and-justice/
[82] Morgan Klaus Scheuerman, Stacy M. Branham, and Foad Hamidi. 2018. Safe Spaces and Safe Places: Unpacking Technology-Mediated Experiences of Safety and Harm with Transgender People. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW (Nov. 2018), 155:1–155:27. http://doi.acm.org/10.1145/3274424
[83] Alfred Schutz. 1967. *The Phenomenology of the Social World.* Northwestern University Press.
[84] John S. Seberger, Irina Shklovski, Emily Swiatek, and Sameer Patil. 2022. Still Creepy After All These Years:The Normalization of Affective Discomfort in App Use. In *CHI Conference on Human Factors in Computing Systems*. ACM, New Orleans LA USA, 1–19. https://doi.org/10.1145/3491102.3502112
[85] Sanhita SinhaRoy. 2021. Defenders of Patron Privacy. *American Libraries Magazine* (Sept. 2021). https://americanlibrariesmagazine.org/?p=125620
[86] Latanya Sweeney. 2013. Discrimination in Online Ad Delivery. *arXiv:1301.6822 [cs]* (Jan. 2013). http://arxiv.org/abs/1301.6822 arXiv: 1301.6822.
[87] Jakita O. Thomas, Nicole Joseph, Arian Williams, Chan'tel Crum, and Jamika Burge. 2018. Speaking Truth to Power: Exploring the Intersectional Experiences of Black Women in Computing. In *2018 Research on Equity and Sustained Participation in Engineering, Computing, and Technology (RESPECT)*. 1–8. https://doi.org/10.1109/RESPECT.2018.8491718
[88] Konstantina Vemou and Maria Karyda. 2013. A Classification of Factors Influencing Low Adoption of PETs Among SNS Users. In *Trust, Privacy, and Security in Digital Business (Lecture Notes in Computer Science)*, Steven Furnell, Costas Lambrinoudakis, and Javier Lopez (Eds.). Springer, Berlin, Heidelberg, 74–84. https://doi.org/10.1007/978-3-642-40343-9_7
[89] Jessica Vitak, Yuting Liao, Mega Subramaniam, and Priya Kumar. 2018. 'I Knew It Was Too Good to Be True": The Challenges Economically Disadvantaged Internet Users Face in Assessing Trustworthiness, Avoiding Scams, and Developing Self-Efficacy Online. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW (Nov. 2018), 176:1–176:25. https://doi.org/10.1145/3274445
[90] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L. Mazurek, Manya Sleeper, and Kurt Thomas. 2022. SoK: A Framework for Unifying At-Risk User Research. In *2022 IEEE Symposium on Security and Privacy (SP)*. 2344–2360. https://doi.org/10.1109/SP46214.2022.9833643 ISSN: 2375-1207.
[91] Mark Warner, Andreas Gutmann, M. Angela Sasse, and Ann Blandford. 2018. Privacy Unraveling Around Explicit HIV Status Disclosure Fields in the Online Geosocial Hookup App Grindr. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW (Nov. 2018), 181:1–181:22. http://doi.acm.org/10.1145/3274450
[92] Reg Whitaker and Reginald Whitaker. 2000. *The End of Privacy: How Total Surveillance Is Becoming a Reality.* New Press.
[93] Meredith Whittaker, Meryl Alper, Cynthia L. Bennett, Sara Hendren, Liz Kaziunas, Mara Mills, Ringel Morris Meredith, Joy Rankin, Emily Rogers, Marcel Sala, and Myers West Sarah. 2019. *Disability, Bias, and AI.* Technical Report. AI Now Institute.
[94] Daricia Wilkinson, Moses Namara, Karla Badillo-Urquiola, Pamela J. Wisniewski, Bart P. Knijnenburg, Xinru Page, Eran Toch, and Jen Romano-Bergstrom. 2018. Moving Beyond a "One-size Fits All": Exploring Individual Differences in Privacy. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems (CHI EA '18)*. ACM, New York, NY, USA, W16:1–W16:8. https://doi.org/10.1145/3170427.3170617 event-place: Montreal QC, Canada.
[95] Pamela Wisniewski, Arup Kumar Ghosh, Heng Xu, Mary Beth Rosson, and John M. Carroll. 2017. Parental Control vs. Teen Self-Regulation: Is There a Middle Ground for Mobile Online Safety?. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW '17)*. ACM, New York, NY, USA, 51–69. https://doi.org/10.1145/2998181.2998352 event-place: Portland, Oregon, USA.

[96] Jill Palzkill Woelfer and David G. Hendry. 2010. Homeless Young People's Experiences with Information Systems: Life and Work in a Community Technology Center. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. ACM, New York, NY, USA, 1291–1300. https://doi.org/10.1145/1753326.1753520

[97] Richmond Y. Wong and Deirdre K. Mulligan. 2019. Bringing Design to the Privacy Table: Broadening "Design" in "Privacy by Design" Through the Lens of HCI. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–17. http://doi.org/10.1145/3290605.3300492

[98] Shoshana Zuboff. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (1 edition ed.). PublicAffairs, New York.

# A INTERVIEW PROTOCOL

## A.1 General Approach to Privacy/User Data

(1) Tell me about your position at <library>. What are your responsibilities?
(2) Tell me about <library>. Describe its mission and goals.
  (a) How would you describe the communities you serve? (Probe: demographics, patron goals/interests)
(3) Can you give me an example/tell me the story of a time when someone was concerned about their privacy in relation to their activities at the library? Probe for other examples.
(4) What are some of the privacy challenges that your patrons/users face when trying to access your services (books, internet, etc)? Explain.
(5) Please tell me about <library's> privacy policy. (Follow up with any questions that arose from privacy policy review)
(6) What kind of platforms or tools does <library> provide?
  (a) Tell me about <Internet platform/tool supported by library>. What's it for?
  (b) Do you use <tool/platform>? Tell me about how/why you use it?
  (c) How do other people use <platform/tool>?
(7) When people sign up for an account:
  (a) Is an email address required? Why or why not?
  (b) Is a username required? Why or why not?
  (c) Is other user data required? Why or why not?
  (d) What kind of information is displayed about users of the library to other people as a default? Where is it displayed (e.g., records, logs, etc.)? Who has access? Where is it stored? How long is it stored? Why? Why is displaying this important for your users or library's goals? Can the defaults be changed?
(8) Can people use <platform/tool/library> anonymously? Pseudonymously? How would users accomplish this?
  (a) How do you define anonymous?
  (b) Does this apply to patrons/users who are using the internet?
(9) Are you familiar with Tor or similar tools?
  (a) Can you explain to me what Tor is used for so that I understand how it's being used?
  (b) Has your library adopted Tor or similar privacy tools? Why/why not?
  (c) Do users of Tor or other such tools have the same access as other users? Why or why not?
  (d) Do you think it's important for <library> to give access to people using anonymous tools like Tor? Why or why not?
(10) How do you educate patrons about their privacy?
  (a) Are their resources for them to protect their privacy? Probe: In the library? on the internet? How do they learn about those resources?
(11) Is there anything important that we haven't talked about related to how patrons use your services?

## A.2 Perceptions of Threats

(1) What are some of the things people do at <library> that can cause problems? Can you give me an example?
  (a) Why is that a problem?
  (b) If applicable: Why do you think they did that?
  (c) What was the impact to <library>?
  (d) How did you resolve <this situation>?
  (e) How is <this situation> typically dealt with?
  (f) Do you have policies in place to address <this situation>?
  (g) What about technological controls or solutions to <this situation>?
  (h) *If no solutions:* Have you ever discussed potential solutions?
(2) *Review all the threats described and ask:* Are there any other you can think of?
(3) *List all threats, again:*
  (a) What are the most critical to address? Why?
  (b) What do you think your library can address?
  (c) Which do you think are easiest/hardest to address?
  (a) What types of patrons have more/less challenges? Explain.
  (b) What are the most critical to address? Why?
  (c) How do you address those challenges?
  (d) Which do you think are easiest/hardest to address?
(4) How does <library> set security related policy? (Probe: Who is involved? How often do they meet?)
  (a) Can you describe a recent security policy discussion you were involved in? What happened?
  (b) How do you educate or inform patrons about these policies?
  (c) Probe: How do those different types of patrons we discussed earlier factor into these discussions, if at all?
(5) Has <library> ever been the target of a cyberattack or data theft? How do you think this has affected your approach to security?
(6) What is your current policy when government information requests are made?
  (a) Have you always had that policy?
  (b) *If no:* When did it change? Why?
  (c) How effective is that policy?
(7) Has your library ever received a request for National Security Letters? Could you explain the circumstance?
  (a) How did you resolve <this situation>?
  (b) What was the impact? (Probe: Changes to policy informal/formal?)
  (c) In the future, how will you address these requests? How, if at all, is that different than in the past?