How We Define Privacy Literacy: Teaching Experiences & Challenges of Community-Engaged Privacy Educators

Tanisha Afnan
University of Michigan
tafnan@umich.edu

Sheza Naveed
University of Michigan
shezan@umich.edu

Griffin Christie
University of Michigan
griffc@umich.edu

Jackie Hu
University of Michigan
yuuhu@umich.edu

Byron M. Lowens
Indiana University at Indianapolis
bylowe@iu.edu

Allison McDonald
Boston University
amcdon@bu.edu

Florian Schaub
University of Michigan
fschaub@umich.edu

Abstract

This study examines the pedagogical approaches and experiences of community-engaged educators—individuals who teach privacy, online safety, or security to specific communities through community organizations, companies, or local institutions, such as libraries. We draw on interviews with 21 such educators across the United States and find that, unlike some privacy and security advice that may emphasize knowledge retention of common skills and strategies, these educators prioritized teaching for independent decision-making. Our participants conceptualized privacy literacy as a process for taking informed action, and, from their insights, we identified five core competencies of privacy literacy: (1) data fluency, (2) account security, (3) fraud detection, (4) information vetting, and (5) surveillance capitalism. Notably, these competencies integrate privacy, security, and online safety concepts into privacy literacy—reflecting an increasingly integrated threat landscape. Embedded within the communities they serve, these educators shared their deep understanding of their students' needs, which varied dramatically, and shared ways in which they tailored their programming accordingly. However, educators also shared significant teaching constraints, including limited time, resources, and organizational support. We discuss the implications of our findings for privacy literacy and for supporting community-engaged privacy literacy efforts.

Keywords

Privacy, privacy literacy, privacy education, security education.

1 Introduction

As digital technologies become more embedded in everyday life, individuals must navigate an increasingly intricate web of online interactions, including financial data management, healthcare administration, and social engagement.

As this reliance on digital services increases, so do the risks associated with personal data collection, surveillance, and exploitation. Personal data is routinely collected, tracked, and monetized, often without sufficient informed consent, leaving users vulnerable to exploitation [18, 27]. For example, in 2023, the FBI's Internet Crime Complaint Center (IC3) reported losses exceeding 12.5 billion due to online scams and cybercrime, with a significant portion targeting vulnerable populations [46].

While data breaches and online surveillance have fueled public concern, privacy literacy remains critically underdeveloped [16, 72], leaving many individuals without the necessary skills to protect their information. Prior studies suggest that despite the availability of privacy resources, individuals—particularly those from at-risk populations—turn to informal channels to learn about security and privacy advice [15, 51, 57]. This reliance on informal sources highlights the importance of community-engaged educators, such as public librarians and volunteers at senior recreational centers and other community organizations, who serve as both trusted peers and authoritative sources of knowledge within their communities. Their proximity to the populations they serve enables them to provide privacy education that is both contextually relevant and accessible.

Indeed, certain communities face disproportionately heightened privacy risks. For example older adults, increasingly rely on digital healthcare services, which often involve managing sensitive personal information online. However, they often lack the digital literacy skills needed to protect their data [24]. Similarly vulnerable are undocumented immigrants, sex workers, and survivors of intimate partner violence, all of whom face privacy threats that current solutions fail to address [11, 26, 38, 55]. These disparities highlight the urgent need for privacy initiatives tailored to vulnerable populations, equipping them with the tools to navigate an increasingly data-driven world.

Recognizing the importance of online access and digital skills, efforts to promote digital literacy have expanded significantly. in both informal and formal educational contexts [19, 36, 54]. However, these initiatives often focus on general technical skills while neglecting privacy literacy, leaving many individuals without the knowledge needed to safeguard their personal data. The American Library Association (ALA) defines digital literacy as "an individual's

Proceedings on Privacy Enhancing Technologies 2026(1), 552–566

https://doi.org/10.56553/popets-2026-0028

ability to find, evaluate, and communicate information by utilizing typing or digital media platforms" [6]. While this definition emphasizes information access and evaluation, it does not explicitly address privacy, security, or data protection considerations, highlighting a critical gap in current digital literacy frameworks. As a result, individuals may develop proficiency in using digital tools without gaining the necessary skills to protect their personal information from misleading data policies and opaque consent models, further complicating their ability to make informed decisions about their personal information. Addressing this gap requires a more holistic approach to digital literacy that integrates privacy and security education alongside foundational technical skills. Without privacy and security education, individuals remain at greater risk of having their personal data misused.

More recent scholarship reveals the deeply contextual and intersectional nature of privacy, through which we now understand how different individuals and communities often hold profoundly divergent privacy needs and concerns [39]. This allows us to identify and acknowledge the various factors that contribute to our individual understandings of privacy, such as age [28, 71], gender [9, 63], or ethnicity [8], but it can also complicate efforts to teach relevant privacy and security topics. Unlike teaching for digital literacy, for which multiple established learning frameworks, resources, and models have been developed, education for privacy literacy remains a more nebulous venture often characterized by ad-hoc efforts.

In this study, we investigate the perspectives of educators currently working to teach privacy literacy to and within specific communities. Leveraging a qualitative approach, we conducted semi-structured interviews with 21 community-engaged educators across the United States who had designed, developed, and led trainings on various privacy and security topics for different communities. For the purposes of our work, we define community-engaged educators as individuals working in organizations, companies, and local institutions that offer support services to community members, specifically through online safety, privacy or security education. Many of our participants were not pedagogically trained as teachers but saw the need and offered their support to community members as a secondary function of their jobs. Our interviews centered on understanding the educators' experiences, challenges, and motivations with the goal of promoting privacy literacy. Our study focused on the following research questions:

- How do community educators define and think about privacy literacy?
- How do educators at community organizations teach others about privacy and security topics?
- What motivations do educators at community organizations have for teaching others about privacy and security topics?
- What constraints, challenges, or limitations do community educators face when teaching for privacy literacy?

Our findings both corroborate and contrast with prior literature examining privacy literacy. Participants in our sample largely identified privacy literacy as the development of abilities and awareness to foster independent, informed decision-making with regards to one's personal information. While this differs from some prior research that typically describes privacy literacy as a static knowledge base [7], it aligns well with previous qualitative explorations in representing privacy literacy as a more fluid concept [32, 72].

Additionally, participants in our sample identified five core competencies they believed were requisite "baseline" knowledge for achieving privacy literacy, including an understanding of *(1) data fluency* (e.g., lifecycle of personal data from collection to storage), (2) *account security* (e.g., password hygiene, multi-factor authentication, etc.), (3) *fraud detection* (e.g., identifying, preventing, and recovering from financial harms), (4) *information vetting* (e.g., combating misinformation and developing healthy skepticism), and (5) *surveillance capitalism* (e.g., understanding how personal data can be exploited and for what purposes). Notably, these competencies integrate privacy, security, and online safety concepts into privacy literacy, reflecting the realities of the increasingly integrated threat landscapes experienced by the audiences of our participants. All our participants, were deeply embedded in and engaged with their communities and uniquely equipped to understand and anticipate the particular needs of their students. However, they also shared obstacles and constraints they faced in their work. In particular, participants highlighted various time, resource, organizational, and audience constraints that limited their teaching efficacy.

We make several recommendations to address these limitations, and discuss strategies to further bolster community-engaged privacy literacy education.

2 Related Work

In this section we examine prior attempts to define privacy literacy, research that highlights the need for more identity- and community-specific privacy education initiatives, as well as ongoing efforts towards educating individuals on relevant privacy literacy topics.

2.1 From Individual Privacy Needs to Systemic Gaps

In recent years, researchers have investigated the privacy attitudes, behaviors, and concerns of individuals across diverse demographic and socioeconomic backgrounds globally [14, 38, 41–43, 61, 62, 70]. Within the United States, prior studies have examined privacy concerns and practices in various at-risk communities based on factors such as age [74], gender identity and sexual orientation [25, 34, 63], culture and politics [4, 53], immigration status [26, 65, 69], and specific vulnerabilities tied to activism, justice involvement, or trauma, such as incarceration [47, 48], homelessness [66], and experiences of intimate partner abuse [37]. Through interviews and focus groups, these studies have highlighted that privacy needs are often identity-specific and vary significantly across different groups. For example, older adults may benefit from educational efforts focused on password hygiene and privacy settings [74], while survivors of intimate partner abuse need help with digital account security [37], and undocumented immigrants may benefit from privacy education conducted in their primary languages and using technology with minimal identity exposure [26].

Despite this growing body of work, Acquisti et al. argue that existing privacy solutions continue to place disproportionate responsibility on individuals rather than addressing the underlying systemic nature of privacy challenges [2]. This persistent imbalance

reflects a need for more comprehensive interventions that incorporate both behavioral solutions and broader regulatory change. In response, our study shifts focus to the perspectives of privacy and digital literacy educators across diverse communities in the U.S.—each with unique demographics, cultural contexts, and specific privacy vulnerabilities. By interviewing community-engaged educators, we aim to address the immediate challenges in enhancing privacy within communities while informing policy changes that may provide longer-term, systemic privacy solutions.

2.2 Defining Privacy Literacy

Privacy has been described as "a concept in disarray" [67], and one especially dependent on context [1, 45]. More recent approaches towards understanding digital privacy acknowledge its variation based on the social, cultural, and political norms of users. By conceptualizing privacy as a monolith, something that is experienced universally, groups whose personal characteristics deviate from the majority may find privacy scholarship, design, and interventions tailored in a way that is unrepresentative and ill–fitting of their own unique needs. Rather, it has been recommended that privacy, and by extension, privacy literacy, be viewed as pluralistic—receptive and accommodating to the existence of many, diverging definitions of privacy and its associated concerns, behaviors, and experiences [64].

Existing scholarship on defining the concept of privacy literacy remains limited. Empirical studies examining privacy literacy typically conceptualize privacy literacy as either a possession of specific declarative or procedural knowledge, or a combination of both [7, 49, 50]. Declarative knowledge relevant to privacy literacy can be understood as a user's awareness of institutional data collection, use, and management practices, their understanding of the legal landscape and regulations that protect their online privacy, and specific technical details [49]. By contrast, procedural knowledge typically refers to an individual's application of behaviors considered privacy enhancing, such as adjusting privacy settings within a browser or online platform, opting-out of targeted advertisements, or engaging in particular digital hygiene practices [7].

Prince et al.'s 2023 study assesses the declarative knowledge of participants through the use of true or false questions that focuses on online privacy laws and rights, and similarly defined and tested for relevant procedural knowledge by checking whether or not participants employed "different protective coping strategies" [50] like ad blockers, manipulating browser privacy settings, or using software that prevents online monitoring. In Bartsch & Dienlin's study, the authors acknowledged declarative and procedural knowledge as the building blocks of privacy literacy, but chose only to measure a user's privacy regulation experience (i.e., frequency of changing privacy settings on Facebook), social privacy literacy (i.e., confidence in adjusting particular settings), and social privacy behaviors (i.e., how accessible different portions of a user's profile were to other users) [7]. Other work, such as Park's 2013 study, focused only on declarative knowledge such as "technical familiarity, awareness of institutional practices, and policy understanding" [49]. Although empirical analyses of privacy literacy diverge in how they choose to measure and define their variables, they tend to agree that the concept is predicated on the understandings (declarative) and behaviors (procedural) of users.

Qualitative studies investigating the concept of privacy literacy, instead, envision privacy literacy as an extension of an individual's critical thinking skills [32, 72]. For example, Kumar et al. utilize Helen Nissenbaum's theory of contextual integrity as a framework [45] for understanding privacy literacy as a cognitive process dependent on the norms and conditions that compete for influence within an individual's given socio-technical context [32]. The authors also argue that privacy literacy should be viewed as a fluid concept that can change from individual to individual and from situation to situation. Moving away from a knowledge-based conceptualization of privacy literacy allows individuals a greater degree of autonomy as they are now capable of interrogating the conditions that impact a situation's informational flows. Wissinger also likens privacy literacy to a cognitive process and believes that it should address five steps commonly featured in critical thinking literature: "understanding, recognizing, realizing, evaluating and deciding" [72]. Wissinger asserts that being equipped with these steps would lead to more competent, privacy-informed decision-making as individuals would become more capable of taking inventory of the risks and rewards presented in a given scenario themselves rather than becoming overly reliant on static rules, which are subject to change, in the constantly evolving digital world.

2.3 Efforts Towards Privacy and Security Education

Individuals' approaches to seeking educational resources related to privacy and security topics can vary tremendously, as they are shaped by their past experiences and perceptions of online safety. In Ion et al.'s study comparing security practices of experts and non-experts, the two groups approached their security practices with different sets of priorities [29]. Experts typically prioritized behaviors like installing updates, using password managers, and two-factor authentication, while non-experts engaged in practices like using anti-virus software, clearing their cookies, and changing their passwords frequently. Experts frequently cited cybersecurity 'best practices' as their source for these practices, while non-experts gravitated towards methods that were the most accessible [29].

Regarding the quality of security and privacy guidance available on the web, Redmiles et al. evaluated articles using three factors: comprehensibility, perceived actionability, and perceived efficacy [58]. Users, both experts and non-experts alike, were then recruited to assess the articles based on the three factors identified. The results of the study revealed that although much of the advice that was vetted was considered both actionable and comprehensible, prioritization remained a key issue, with both experts and non-expert users struggling to determine which actions were most critical to take. The sheer volume of advice and the general lack of clarity on prioritization made it overwhelming for users to decide on a best course of action [58, 59], something we observed with participants in our findings as well.

Of the topics that are typically covered in advice relating to privacy and security concerns online, phishing is an issue that is especially prevalent. In Franz et al.'s study of current phishing interventions, the researchers developed a taxonomy to classify these tools by type (e.g. training, awareness, design) and their intended effect (e.g. increasing awareness, building detection skills)

[23]. Their analysis revealed that an overabundance of phishing interventions exist that could burden users with information overload, rendering many underutilized and forgotten. When examining efforts to teaching for privacy literacy live, Saglam et al.'s work identifies K-12 school teachers as one of the most significant informational sources for children's online safety and cybersecurity [60]. Although parents, governing bodies, and cybersecurity-specific advocacy organizations were identified as important parts of building children's privacy literacy, this responsibility primarily fell on teachers, who often reported being under-resourced and under-educated on relevant topics themselves. Based on their input, Saglam et al. synthesized five broad categories of instruction that school settings typically focused on, including: 1) cyber security technologies (antiviruses, firewalls, encryption); 2) safety protocols (location sharing, password management, online 'ethics'); 3) technical risks (viruses, phishing, hacking); 4) nontechnical risks (inappropriate content viewing, cyberbullying, sexual harassment/exploitation); and 5) privacy awareness (digital footprints, impersonation/identity theft, personal information control).

In a higher education context, Egelman et al. worked to develop the Teaching Privacy Program (TPP) website and curriculum for undergraduate students at the University of California, Berkeley [17]. While the TPP curriculum was developed as a component of a larger research agenda, the research team constructed ten primary principles which they believed were most significant to a student's development as vigilant digital citizens. These principles held some similarities to those identified by K-12 teachers, and were anchored around themes of digital hygiene, managing one's digital footprint, understanding that private corporations are collecting and monetizing the personal data of their users, and that privacy stewardship often falls on the individual as opposed to the government, with a focus on U.S.-centric rules and regulations. In line with Egelman et al.'s work, Švábenský et al.'s meta-analysis of cybersecurity education articles published at SIGCSE and ITiCSE, which are research conferences focused on computer science education, examined topics prioritized by experts as a part of larger ongoing research initiatives. [68]. Of the papers examined by Švábenský et al, a majority of them explored short-term educational interventions (such as labs, practical/hands-on assignments, and educational games) aimed at undergraduates, advanced degree-seeking students, as well as technical professionals already in cybersecurity or adjacent fields. The intended audiences of these interventions gave rise to teaching content that was more technically demanding, focusing on topics such as cryptography, network security and monitoring, cyberattacks, malware, and secure software engineering.

In our study, we contribute perspectives of educators outside of formal academic settings in order to understand the needs, priorities, and demands involved in achieving privacy literacy with students across diverse communities, and with unique privacy considerations. Our work shows how understandings of privacy literacy are operationalized currently at the community level, how it differs from and aligns with the prior work, and what support is needed to support such community-oriented efforts.

3 Methods

There is limited existing work that has examined community-based efforts towards privacy and security education [40, 64], and this study offers a glimpse into the perspectives and realities of the individuals leading this work. In our study, we focused on the experiences of community-engaged educators in the U.S., serving various audiences across different contexts, including small businesses, libraries, and non-profit organizations. None of our participants, who represented a diverse set of academic and professional backgrounds, considered themselves cybersecurity professionals, had conducted privacy or security research, or had taught formal graded courses on privacy and security topics at the higher-education level. Instead, many of them held degrees in education, library sciences, and social work, while a majority of their prior professional experience involved community-service work. Our study investigated their various teaching approaches towards informal education on privacy and security topics, including educators' motivations for leading this work and the challenges they faced. The research team opted for a qualitative research approach to engage more deeply with our participants and gather richer participant insights. To achieve this, the first author led 21 semi-structured interviews with participants via Zoom from November 2023 to March 2024.

The University of Michigan's institutional review board (IRB) reviewed and approved (exempt) our study.

3.1 Study Design

Our interview script[1]was divided into three parts: participants' background and conceptualizations of privacy literacy, their involvement with their affiliated community organization, and questions to investigate their privacy-related teaching experiences and approaches. The interview script included a set of opening questions intended to build rapport, as well as a final set of closing questions to allow participants a chance to share relevant experiences or questions that had not been captured throughout the rest of the interview.

We recruited adult educators working in community-based organizations in the U.S., which we defined as organizations, companies, or institutions providing support services to their community, where at least some part of their role involved teaching individuals about privacy or security topics. Our educators led programming on these topics across the U.S. in environments ranging from public libraries in New York City to neighborhood service organizations in small townships in the Midwest. The 'students' our educators served varied dramatically as well, and ranged from school-age children to older adults and non-English speaking immigrants. Participants were challenging to recruit due to our specific eligibility criteria, but we attempted to gather a sample that reflected reasonable diversity with regards to gender, teaching experience, and teaching context. Eligible participants were initially contacted via email, and then invited to share their availability and schedule a remote interview session with the first author. All interviews were conducted remotely using Zoom, and all interviews were conducted in English. Participants were then directed to a post-study survey via Qualtrics at the end of their interview session (see Appendix A). This survey gathered demographic data to help us contextualize our

[1]See full materials in our OSF repository: https://osf.io/g3p7c; also in Appendix A.

sample. Upon completion of their interview session, participants received a $25 virtual gift card delivered to their personal email. On average, interviews lasted 43 minutes, ranging from 33 to 65 minutes.

3.2 Recruitment and Demographics

We define community-engaged privacy educators as educators working in organizations, companies, and institutions that offer local support services, including online privacy or security education. The research team compiled a list of >30 community organizations across the U.S. that have offered digital skills workshops, with a focus on privacy-relevant topics, using relevant keyword searches (e.g., privacy, online safety, security training) on social media platforms, search engines, and local meetup groups. Team members then identified contact persons at each organization to reach out to by email using a standardized recruitment message. We also recruited participants using social media posts, snowball sampling, and word-of-mouth referrals from local connections to our university. While we selectively recruited participants who had taught privacy or security topics, our study revealed that these topics are rarely taught alone in such settings, and instead are often included within larger digital skills trainings. Our participants did not distinguish between years of teaching specifically on privacy related topics vs. other digital literacy concepts.

Eight of our participants identified as men, while the remaining 13 identified as women. Individuals ranged in age from their late twenties to late fifties, with an average age of 36 years. Participants in this sample were highly-educated; all of them had attended and graduated from college, and 19 of 21 participants held advanced degrees. A majority of participants reported having more than 5 years of experience teaching about technology related topics, and catered to a wide range of audiences, including children, older adults, college students, low-income adults, and immigrants. We recruited across the U.S., and heard from participants in Colorado, Texas, Pennsylvania, Massachusetts, New Jersey, Michigan, and New York. Table 1 provides an overview of participant demographics, including the type of organization with which the educators were affiliated.

Table 1: Participant demographics

ID	Organization Type	Specific Audience(s) Served	Education
P01	Public library	Low-income adults, immigrants, adults (general)	M.A./M.S.
P02	Non-profit org., public library	Older adults, children, adults (general)	M.A./M.S.
P03	Public library, senior centers	Older adults, LGBTQ+ adults, adults (general)	M.A./M.S.
P04	Small business	Adults & children in rural areas	B.A./B.S.
P05	Small business	Older adults, adults (general)	B.A./B.S.
P06	Small business	Older adults, adults (general)	M.A./M.S.
P07	Non-profit org.	Children & adolescents	M.A./M.S.
P08	Public library	Adults (general)	M.A./M.S.
P09	Public library	Affluent adults, older adults, adults (general)	M.A./M.S.
P10	College library	Young adults	M.A./M.S.
P11	Public library	Low-income adults, older adults, children, adults (general)	M.A./M.S.
P12	Public library	Low-income adults, older adults, adults (general)	M.A./M.S.
P13	Public library	Adolescents, older adults, adults (general)	M.A./M.S.
P14	Public library	Low-income adults, older adults, adults (general)	M.A./M.S.
P15	Public library, professional assn.	LGBTQ+ adults, immigrants, domestic abuse survivors, adolescents	M.A./M.S.
P16	Public library	LGBTQ+ adults, adults (general)	M.A./M.S.
P17	Public library	Older adults, adults (general)	M.A./M.S.
P18	Non-profit org.	Low-income adults, ethnic minority adults	M.A./M.S.
P19	Small business	Older adults	M.A./M.S.
P20	Public library	Affluent adults, older adults, children	M.A./M.S.
P21	Academic library	Young adults	M.A./M.S.

3.3 Data Analysis

Positionality. Our research team consists of academic privacy and security researchers, some of whom have experience educating other individuals on these topics in both formal and informal educational settings. Our knowledge on privacy and security advice, as well as past experiences in leading educational workshops contributed to our approach towards analysis and our understanding of the findings. Individuals on this team may be considered 'complete member researchers,' commonly defined as individuals who could be considered peers of the study participants due to common shared experiences, as well as others considered 'peripheral members,' or those who "observe and interact closely enough with [study activities] to establish an insider's identity" [3], due to our experiences teaching others about privacy literacy related topics. The first author, who scheduled and facilitated all interviews, has organized and led educational privacy and security workshops with local service organizations in their community.

Qualitative data analysis. All interviews were audio recorded using Zoom's internal recording feature, and all resulting recordings were transcribed using Otter AI. The team redacted any personally identifiable details from recordings prior to transcription, and transcripts were reviewed by the research team for clarity. Throughout the data collection process, the research team met regularly to debrief on sessions and discuss findings. We utilized a thematic analysis approach in examining the transcripts, field notes, and recordings collected from the interviews, following Braun & Clarke's six-step process [10]. The first author developed the initial codebook using inductive coding across the entire dataset to identify recurring themes. Other members of the team then offered input on these initial themes while also reviewing the dataset to refine preliminary codes.

After iterative rounds of the initial inductive coding, the first and second authors worked together to apply the finalized codebook across each individual transcript. This process was conducted using ATLAS.ti, a qualitative data analysis software. To ensure that this analysis was consistent, both coders independently coded the same transcript and discussed similarities and differences in their coding approach. Both authors continued to code more test transcripts independently, convened to compare codes, addressed discrepancies, and modified the codebook accordingly. After three rounds, we achieved a Krippendorf's alpha value of 0.729 indicating reasonable inter-rater agreement. The final codebook included 20+ parent codes structured around the primary research questions, with several additional sub-codes. The first and second authors then split and coded all transcripts with the final iteration of the codebook.

3.4 Limitations

Our study design has some limitations. Given the focus on an understudied topic, our research questions were exploratory in nature and required a qualitative approach to gather detailed, individual experiences. A semi-structured interview protocol allowed us to collect relevant data, but also introduced a few constraints.

Our study was conducted in the U.S., therefore limiting our findings to the sociocultural norms of the U.S. Care should be taken while generalizing our findings as norms around privacy, digital literacy, and education may vary across the world, even though we focused on recruiting for reasonable diversity within the context of the United States. Additionally, due to the specialized nature of our participants' work, and the difficulty faced in recruiting this niche population, a majority of our participants were librarians, which may have influenced the insights we got from our interviews. We found no significant differences between the experiences shared by participants working in different institutions and organizations than those who primarily worked in a library setting, but further research with a larger sample size could further validate or expand these findings.

4 Findings

In this section, we unpack our participants' experiences and perspectives as educators teaching members of their communities about common privacy and security topics, and share our findings below as an extension of the larger discussion around defining privacy literacy, and the need for more community-engaged privacy education. First, we discuss participants' motivations for teaching privacy literacy, as well as what privacy meant to them. We then expand on current concepts of privacy literacy by sharing our participants' ideas of what it means to be privacy literate, including five core competencies they identified as essential components of privacy literacy: (1) data fluency, (2) account security, (3) fraud detection, (4) information vetting, and (5) surveillance capitalism, with an emphasis on instilling independent decision-making. Notably, these competencies incorporate privacy, security, and online safety aspects into a broader conceptualization of privacy literacy.

Next, we discuss the teaching approaches of participants, including ways they design, develop, and tailor material for different audiences and concerns. Our participants emphasized the importance of including specific, real-world scenarios that reflected the needs of their communities, setting aside time for individual questions and support, live demonstrations, and hands-on activities as the most effective educational strategies. Although numerous cybersecurity educational resources have been developed by researchers and other professionals, we find that educators in our study tended to rely on their own knowledge, and the knowledge of those around them, to support their students within their informal learning environments. Lastly, we discuss the struggles and limitations our participants faced within the contexts of their roles, including time, resource, audience, and organizational constraints.

4.1 Community Welfare and Teaching Motivations

Our educators led digital skill trainings on online safety, privacy, and cybersecurity topics across the U.S. These environments ranged from public libraries in New York City to neighborhood service organizations in small townships in the Midwest. The students our educators served varied dramatically as well, and ranged from school-age children to older adults and non-English speaking immigrants (see Table 1). Most of our participants offered classes or trainings as one-time, small group offerings rather than multi-class series. Classes were typically structured as introductory overviews to certain privacy and security topics. Class times varied in length, but mostly consisted of one-hour sessions, which were offered with limited frequency (i.e., generally 'as requested' or on a quarterly basis). However, there were exceptions to this format, such as P12 and P14 who worked in more well-resourced libraries, and could offer regular open lab time (*"kind of a freestyle learning environment where people can come in and work and ask questions [to] get some advice"* –P14), or P9's weekly "Tech Tuesday" classes that each focused on one specific topic in particular (e.g., a dedicated hour-long class on misinformation). Other participants who operated under small businesses and non-profit organizations also had slightly more flexibility as they usually offered their services to local clients who might be looking to troubleshoot specific concerns with slightly larger windows of time.

Over half of our participants reported that their role as educators, or time spent actively teaching, was a non-essential function of their job. Instead, many shared that they volunteered to lead this programming, usually offered as a free service by their larger organization, as an optional, secondary task. When asked what drove participants to engage in this work, a vast majority of educators described these efforts as a means of giving back to their community, empowering their students, and, as participants in our sample were typically embedded into the neighborhoods they served, even occasionally supporting their own friends and acquaintances. P18 shared their rationale for both founding their neighborhood organization and providing education on privacy topics for residents:

> "I live here. I'm a long term resident. My family has been in this neighborhood since 1946. I'm the founder and CEO. So, I lead the organization, come up with ideas in partnership with residents and other team members. We together, we work to come up with different programs based on the needs of the residents." (P18)

The unique position of our participants as both community members and educators, allowed them to better understand the pressing digital needs of their communities, and created a greater sense of investment in the learning outcomes of their students, with the goal of achieving privacy literacy.

4.2 Meaning of Privacy

We began our interviews by asking participants what privacy meant to them. Our participants' understanding of privacy provides context for how they defined and thought about privacy literacy, which we discussed after.

While participants' understanding of privacy varied in nuanced ways, their general conception of privacy was similar. Generally, for our participants, privacy meant having control over what information they share and with whom. For instance, P03 described privacy as *"the ability to have control over your data and information*

and decide how to use it." Some participants specifically emphasized control over what is made public, such as P07: *"I think the ability to keep private information separate from a public, separate from bots, separate from hackers."* To some participants, this meant keeping their name off the internet:

> "So I really try not to leave very much of a digital footprint. Because it's scary how much information you can get. So for me, privacy is I'm trying to keep my name off the internet. Yep. But also to I'm careful with my own privacy, like even at work, our supervisor would like to have our photos on our website for work. I'm not comfortable with that." (P11)

For others, privacy was more about who specifically has access to their information: *"I have control over and get to make decisions about who has access to any information related to me;"* as well as about transparency: "Privacy in a digital space [...] it comes down to that control aspect. And also transparency, like knowing who's got access to what" (P20).

Many also connected privacy with agency, as expressed by P02: *"privacy means being able to opt into services instead of opting out of them. And [...] having authority over what is accessed by who."* This also ties in to the value of privacy as it is seen as a right, not a privilege:

> "Privacy is like, [how] am I going to put it, let me see. Oh, privacy is a right, is a human right. [Without] privacy you [can't] have the freedom of association, freedom of thought, freedom of expression, as well as freedom from discussion. But it's also privacy is quite hard to define. Because you know, the different countries, different ethnicities offer different views when it comes to privacy as individuals. Yeah, well, for me, privacy includes the rights to be free from interference, intrusions." (P04).

Overall, our participants' understanding of privacy aligns with general definitions of privacy and reflected common privacy concepts and values, such as privacy as control, the notion of agency, and privacy as a human right.

4.3 Privacy Literacy, Defined by Educators

As discussed previously, our participants would not be generally considered cybersecurity 'experts', though they were technically skilled in everyday digital contexts. This provides a contrast to the perspectives typically represented in conversations around defining privacy literacy, most often by computer science researchers. Despite the deep variation in participants' teaching contexts, we found similarities in how they conceptualized privacy literacy, and what they stressed to their students in helping them gain privacy literacy. Rather than an emphasis on knowing and retaining specific information, educators felt that their students could be considered 'privacy literate' when they were able to effectively understand motivations for protecting their privacy, and react assertively to privacy risks in accordance to their own needs and preferences. P7 shares that achieving privacy literacy could mean simply having *"the ability to make choices in your digital life, and where information that is personal and distinguishes you from another person can be kept as personal as you'd like."* P14 shared a similar sentiment, stating that for them, as an instructor helping students *"overcome their trepidation or their fear, and kind of build confidence is really the number one"* priority in teaching about privacy and security topics.

The distinction between privacy and security was also highlighted by many of our educators, as P21 differentiated the two:

> "We're thinking about digital privacy as [...] the right to own information about our lives and the right to have that be private. I think a lot of times people in like instructional contexts, we often kind of use [the term] interchangeably with the term security, which is more about protection." (P21)

At the same time, in their educational efforts, all our participants included security strategies in their programming as practical advice, which they viewed as necessary and relevant for fostering a deeper conceptual understanding of privacy management given today's online threats. Educators shared how the topics they have taught in relation to privacy literacy had evolved over time as platforms, systems, and devices continued to rapidly change. For example, P9 shared how much of the security advice they shared with students when they first led trainings in 2012 centered around desktop computer risks, such as malicious viruses, while new material now instead focuses on smartphone security as community members have shifted towards a greater usage of mobile devices. As a result, participants identified continued individual motivation as a key characteristic for achieving privacy literacy. For instance, P17 likened privacy literacy to any other form of literacy, rather than a rubric of static knowledge checks.

> "I think I would say a big part of privacy literacy would be like being literate, and understanding why it matters, or why you're talking about privacy in the first place. Again, [I don't know] if when we're talking about digital privacy, it'd be [specific] things like ads and passwords, or whatever it would be [...] instead, I think literacy, in most things, is sort of an ongoing learning process. I think part of it is just having enough scaffolding to take in new information." (P17)

Largely, participants steered away from the empirical perspective of confining privacy literacy to discrete buckets of knowledge [7, 49, 50], but instead were more aligned with prior qualitative investigations that conceived of privacy literacy as a way of thinking and acting critically [32, 72] in order to increase real-world relevance for their audiences. Though most of our educators agreed that being privacy literate had more to do with developing strong problem solving abilities, participants still felt there was some "baseline" knowledge individuals had to be familiar with, including an understanding of common terminology, threats, and security strategies, to be considered privacy literate. Due to the diversity of audiences served, environments taught in, and a lack of standardized educational materials, we saw variation in what topics, skills, and strategies participants highlighted to their students. For example, in audiences that primarily consisted of older adults who abstained from social media, material related to social media privacy was omitted, while the opposite was true for educators that mostly catered to children and adolescents. Ultimately, participants placed an emphasis on teaching students what to be aware of with regards

to privacy in order to support individual decision-making, rather than on rote memorization.

From participants' conceptions of and approaches to privacy literacy education, we identified five core competencies, based on their prevalence and significance to building a conceptual understanding of privacy: data fluency, account security, fraud detection, information vetting, and surveillance capitalism. Across participants these competencies were described as essential to being considered privacy literate. Interestingly, these competencies combine and integrate privacy, security, and online safety aspects that in the literature are often treated separately, yet, our participants related them all to privacy literacy, reflecting the increasingly integrated online threat landscape that their communities faced. Next, we discuss each of them in more detail.

4.3.1 First competency: data fluency. First, participants felt their students needed a basic understanding of the data life cycle, including knowledge of how their personal data is created, stored, shared, used, or destroyed. P1, in their classes, stresses this as the most important and essential learning outcome for their students.

> "I think, you know, those principles [of data fluency] are the most important thing. Just sort of understanding how the internet works, especially the fundamentals of data [...] Data in transit, data at rest, what entities could sort of, you know, see the data as it was in transit along the way..." (P1)

Educators stressed that a stronger understanding of how their personal data exists on the internet gave students more confidence in then exploring ways to take relevant actions, such as requesting data to be removed or deleted, and in general encouraged individuals, who otherwise felt overwhelmed, to be more proactive in managing their own information. P15 shares an interactive activity they led recently to better illustrate these concepts:

> "I'm not your tech support, [but things I can teach] are, you know, teaching people about data lifecycles. What it looks like to understand, 'Are there retention periods?', 'Like when are you deleting data?' You know, we did a shredding party recently. So we got the shred bins and got some snacks and just told people like, 'Hey, this is an opportunity to go through your files and get rid of any, you know [unwanted information]' and we had a bunch of people come and you know, dump boxes into the shred bins." (P15)

4.3.2 Second competency: account security. Second, all 21 participants recounted having dedicated material related to password hygiene and secure account management. Participants emphasized the need for all their students to be able to create and safely store strong passwords, use additional verification layers (e.g., multi-factor authentication), as well as physical strategies to keep personal devices safe (e.g., using a webcam cover on a personal laptop). While this topic centers largely around *security* strategies, it was seen as essential to preserving one's privacy online, and therefore highlighted as a core competency. P13 shares how they present account security strategies after first relaying their relevance.

> "[For my students], I would want to know, you know, do they think they're safe? Like, do they think that their information online is private and protected? That would probably be an open question. And then [I'd ask] about, 'do you know about the different types of ways of protecting your information?', you know, multi-step authentication and password generators, just sharing all the different things." (P13)

These skills were especially top of mind for educators who served older adults, whom multiple participants identified as less likely to adopt secure password managers and multi-factor authentication options, as well as more likely to reuse the same password across accounts. As an example of the adaptive strategies participants used, P14 shared how they abandoned the idea of forcing their reluctant students to adopt a password manager, and instead walked through physical strategies for secure password storage *"because the pen and paper method is preferable for a lot of [their] students*."

4.3.3 Third competency: fraud detection. Third, participants felt that individuals should be confident in their ability to identify and protect themselves from fraud and scams online. In their 2022 typology of privacy harms, Citron & Solove identify *economic* harms as one of the seven major harm categories, and define it as monetary losses or "the loss in the value of something," which additionally contributed to feelings of privacy violation [12]. This was also relayed in interviews as one of the most requested topics by students across all environments, who often shared their fears and concerns with the class. Additionally, fraud and scam detection was stressed as one of the most context-dependent vulnerabilities, as various factors such as age and socioeconomic status were believed to have deeply influenced one's risks for falling prey to economic harms. P19 considers how these factors may affect a student's vulnerability:

> "People who have past interactions with the carceral system, undocumented people, people who go to poor schools, people who are trans people, people who have any remotely transgressive seeming [identities] might have to worry more. [...] If I were going to a senior center to talk about like, basic privacy, or whatever I would definitely talk about scams." (P19)

Some educators shared that students became overly panicked when confronted with online scams, and benefited most from being encouraged to stop, take inventory, and think clearly before immediately reacting to stressful situations. To further account for individual or community specific concerns of their students, educators guided students through concrete real-world scenarios that were of particular relevance to them. This was seen as especially useful in helping students recognize some of the common hallmarks of scams when making financial decisions, and leading them to use their own deductive reasoning to protect themselves. P8 shares how they used this approach to help students assess housing offers online:

> "It's really kind of case by case. So if someone needs to find a place to live, we're helping walk them through that. They might be on Craigslist and see these ads that we know are obviously scams, so then [it's more about] kind of talking to them, and talking them

through why we think that. We don't make the decision for them. But talk through why [it] might not be good to follow up on." (P8)

Many of our participants also pointed out the constantly evolving nature of scams, including their increasing sophistication and various modes of delivery (e.g., scams utilizing deepfake technology for impersonation purposes on social media). To prepare students to feel confident in this competency, participants placed an emphasis on spotting scams and fraud before sustaining real harms, rather than on recovering resources following a scam, which some educators felt was more complicated and difficult to teach.

4.3.4 Fourth competency: information vetting. In a similar vein, several educators were also concerned about the rise in misinformation online, and consequently the ability to vet information online for its veracity was highlighted as the fourth core competency. Although information vetting and scam detection may appear to be closely related, our participants made clear distinctions between the two, with financial harm and identity theft recovery being unique to scam detection, while information vetting was instead linked to online safety and identifying inaccurate, misleading, or biased content. Misinformation, and the public's belief in it, remains prevalent in political, health, and science debates [22]. The rapid growth of social media in spreading misinformation, along with the emergence of AI technologies that can generate and disseminate fake content, has worsened the problem [5]. Participants shared that students should be able to accurately distinguish between truthful and false information, as well as between legitimate and deceptive sources; otherwise, they risk misinformation, manipulation, and harm. P13, who has attempted to create material focused on misinformation, noted:

> "Learning kind of what misinformation or disinformation is is [super important]. It's really easy to fall victim to bad information. [...] A lot of it is just showing them you know, this is how you can spot misinformation, this is how you can kind of protect yourself, or go to fact checkers, or if you're not sure, and it seems fake, it probably is fake." (P13)

For several participants, instilling skepticism in their students was a key component of this competency, as members of their community could be overly trusting of all information encountered online. This was a barrier that proved to be challenging to overcome for some participants, such as P12 who shares that *"getting people to not trust [everything] has been a challenge."* Another participant, P10, explained her approach of teaching information vetting as prompting her students to interrogate sources: *"I would ask them, how do they identify if a news website or source is offering reliable information? How to find out about its bias?"* P10 emphasized to her students that misinformation is not only about factual inaccuracy but also about the ways partial truths can be framed to shape perception.

Together, we saw educators outlining a general process in which students were encouraged to pause when presented with new information, ask questions about the information presented, and consider several factors (e.g., investigating the site or source, taking note of details like typos, etc.) before judging the veracity of the information.

4.3.5 Fifth competency: surveillance capitalism. Lastly, educators identified developing a strong understanding of surveillance capitalism as an essential component to achieving privacy literacy. This was believed to be especially important in motivating students who otherwise lacked an awareness of invasive corporate data use practices to take more proactive measures towards protecting their privacy. Surveillance capitalism, as defined by Shoshana Zuboff, refers to the commodification, by corporations, of people's behaviors, lives, and private experiences captured and collected through their personal data [75]. In teaching basics about managing one's privacy across social media platforms, disabling cookies, or limiting ad tracking, educators also stressed to students *how* social media, and other digital services are able to remain free for use, and *why* it can be important to limit the degree to which one's information is available to private corporations or other users. Many of our participants stated that they did not prescribe specific privacy settings to students, but instead wanted students to be able to manipulate settings and permissions to align with their individual comfort levels once they had established an understanding of potential risks and trade-offs. For example, P6 shares the following:

> "With the population I work with, they ask about their privacy a lot [...]. They know that their information and data is out there, but they don't really know what and how it's being used. [Some will say] 'I don't mind that, you know, someone sees that I shop for men's clothes, and then they show me nice advertisements for new pants or whatever. That doesn't bother me.' But what [does] sort of bother them is when I [...] talked about 'oh, it turns out [some companies] have really detailed psychological profiles that include your agreeableness'. Or the fact that they're using that to deliver political ads. [...] I think that kind of turned some light bulbs on to people because that shows them like, okay, for you, how can your info be used in a fair way versus an unreasonable way?" (P6)

Ultimately, our participants constructed a comprehensive definition of privacy literacy, incorporating concepts of online safety, technical security, and privacy to reflect the multi-faceted risks and challenges faced by the diverse members of their communities.

4.4 Teaching in Informal Educational Environments

Unlike formal educational settings, such as schools or universities, informal learning contexts allow educators the flexibility to create their own materials, and set their own teaching agenda. Unfortunately, this flexibility also comes with the drawback of having limited scaffolding and resources to do so. In developing their trainings, our participants leaned on a variety of resources, strategies, and teaching approaches to support their students.

4.4.1 Knowledge sources for teaching materials. Educators usually identified the topics of highest relevance for their students before engaging in information-seeking practices to design their teaching materials. Some educators shared that they surveyed students who

signed up for sessions ahead of time to identify concerns or current skills, others started with open-ended Q&A sessions to establish group priorities, and some facilitated group discussions in which participants were prompted to share their reasoning for taking a particular class or workshop. For example, P6 often begins sessions with a *"a tech discovery program, where we will survey [students] with a bunch of questions related to their tech skills, how comfortable they feel using certain devices, or performing certain tasks"* to tailor classes accordingly.

However, tailoring sessions to suit the needs of different students was difficult to do consistently, and became a task that many educators struggled to balance with the other demands of their work. P3, for instance, shared the toll the "emotional labor involved in that [work]" took on them, and that while they would love to offer more of their time felt that *"[they] were already at capacity."* Once priorities were established, most commonly, participants relied on their own knowledge to create content for their trainings. Beyond themselves, educators felt most comfortable reaching out to those within their immediate social circles for additional advice, with some borrowing existing material from within their organization, usually developed by colleagues who previously taught in their role, or more 'tech-savvy' friends and family. For instance, P13 leverages a combination of their own knowledge with that of a family member to create their educational materials:

> "My dad works in IT. [...] I'll do my own research. And I'll be like [to my dad], 'Hey, is there anything I'm missing that I need that you think I should focus on?' And he'll send me something back, like, 'No, I think that's a pretty good, broad overview.' A lot of it is just research, and more research, and more research. As far as the ideas, it's hard to come up with ideas and topics for programs. So I'll just kind of take a look through things and then I'll be like, 'Oh, maybe this is something we should do." (P13)

This strategy reflects patterns identified by Rader et al., namely how individuals are more likely to pay attention to, and adopt, security advice introduced to them by peers and real-life connections [52]. From our conversations, some participants reported that though they recognized there was an abundance of privacy and security advice online, it could feel burdensome and overwhelming to peruse all the relevant information available. Additionally, the financial constraints experienced by many of our participants and their organizations, which we discuss in the our final section, meant that some participants were unable to access relevant information behind paywalls, such as specialized scholarly databases.

Still, though less commonly, a few participants named specific online resources they preferred to consult due to their perceived trustworthiness. Notably, the educational materials from the Electronic Frontier Foundation (EFF) [20], and amongst participants who worked in libraries, handouts and templates from the Public Library Association [73]. When teaching about topics for a specific platform or device, multiple participants preferred to consult the source directly, and read the relevant internal FAQs or instructional pages. P9 shares her strategy for utilizing 'in house' resources:

> "If I'm going to do a class on Zoom privacy, I will go to the Zoom help page and the Zoom information [page], and try to organize it in the same way that they do in terms of, you know, 'do this and then do that' [...] And usually then I'll customize it to what I feel that the class needs. So usually the resources I go to are the ones specifically related to the subject at hand. You know, whether that's for iPhone or Zoom or something like that. I don't have a general go-to resource." (P9)

The information seeking practices of our participants reflect both their teaching priorities, in wanting to center material around the most pressing issues of their communities, and the constraints of their teaching contexts.

4.4.2 Session structure and teaching strategies. We also noticed differences in terms of teaching strategies and classroom management approaches across our participants. While there was general agreement on essential competencies for achieving privacy literacy, participants had different learning objectives, ordering of topics, and activities they incorporated into their teaching. For most sessions, educators leveraged an ad-hoc approach, usually adapting their materials and activities to the needs of each group without specifically outlined learning objectives. Our educators, as members of the communities they served, had a deep understanding of the limitations and concerns of their audiences. Students varied greatly in their knowledge and skill level across trainings, and participants typically found it better to adjust materials based on the particular audience rather than sticking to specific scripts.

All educators in our sample typically structured their sessions around a set of lecture-style slides, but a large majority of them agreed that what proved to be most effective in teaching students about privacy and security topics included incorporating hands-on activities (e.g., walking students through privacy policies or settings), grounding material with concrete, real-world scenarios that were relevant to their students' lives (e.g., managing one's social media presence from employers in a group of job-seeking individuals), and including time for one-on-one support and attention (e.g., troubleshooting individual device issues across the classroom). Some participants who had a background in education also mentioned adopting threat modeling exercises, as a means to instill independent decision making within their students. P15 unpacks this concept, and contrasts risk tolerances across different kinds of students they may teach within their community:

> "[We want] people to learn a little bit about different privacy topics. And then to answer some questions, to build a toolkit for themselves, to kind of [support the things] that matter to them knowing that people have different tolerances and needs around privacy. Like, social media influencers are going to have a very different outlook on privacy than somebody who is in a domestic abuse situation, right? And so like, to say there's just a universal blanket understanding of privacy doesn't really work. I think that gets into threat modeling, and all that different sort of stuff too. It's like, where do we fall [on the spectrum], what do you have to risk, and then setting up a system." (P15)

Across these various strategies and approaches, we observed one overarching theme common to all participants: Their trainings and sessions should always focus on the risks and topics most relevant to their students, while minimizing time spent on any others.

4.5 Challenges in Teaching Privacy Literacy

Our participants' vast experiences with privacy literacy education were not without obstacles. Despite their best efforts, the educators shared that they felt their teaching could be significantly more effective if they were not limited by audience constraints (i.e., addressing different priorities of different students within a group setting), organizational constraints (i.e., limitations related to the host organization, such as lengthy bureaucratic procedures for approving teaching materials), time constraints (i.e., limitations related to the length of teaching time available), and financial/resource constraints (i.e., limitations related to what money and resources are available for teaching these topics, such as limited high speed internet access).

Though our participants shared teaching approaches and strategies they recognized as most effective, such as one-on-one support or hands-on activities using participant's own devices, many felt unable to deploy these methods regularly due to the aforementioned constraints. For example, participants largely agreed that providing individualized attention was most effective in reaching students and addressing unique concerns, but, as most facilitators led classes on their own, this strategy became burdensome to routinely offer. This was especially true for audiences in which students had a diverse range of skill levels, which coupled with the oftentimes short and infrequent nature of trainings, meant educators could only keep sessions limited to a group format. P20 shares that *"one on one attention was the most helpful, [and] that sort of sustained, very personal approach is definitely successful"*, but that *"it's also very time intensive [and that] we don't really have a specific team of specialists at our library, we're too small."* Unlike formal educational environments, such as a multi-week college course, most of our educators only taught one-time workshops, usually 1-3 hours in length. P14 identifies time constraints as their largest limitation in teaching about topics effectively:

> "I think what I struggle really with classes like this is that we do have a very small window of time. You know, if this was a classroom setting, like in high school, or in a college, or even an elementary school, you could count on having several hours over the course of a week or a month to kind of do activities, kind of reinforce the ideas and have repetition for learning. A lot of what we do in the library, it's kind of like, 'here's a whole bunch of stuff, here's a few activities you can practice when you get home.' But after that, it's kind of on the learner to write, practice and be self motivated." (P14)

Participants also shared that students who were not particularly tech-savvy lacked an initial interest in learning about privacy and security topics, but that many grew to develop a curiosity *after* hearing about online privacy threats and risks through more general digital literacy programming. For our educators who primarily served communities looking to develop computer skills for job readiness, essential functions, or social connectedness, many felt that they were unable to offer education specifically focused on privacy and security topics. Instead, those participants shared that they felt relegated to offering small pieces of privacy literacy programming within other workshops and trainings about broader digital literacy skills.

Some of the educators serving these communities shared instances when they offered more targeted trainings related to privacy literacy, but unfortunately observed that those workshops typically had lower student attendance and interest, discouraging them from leading future targeted sessions. For example, P11 shared the ways they combined the skills their students were most interested in with additional coverage on privacy and security topics in their classes:

> "People are very digitally illiterate. I was in a county that had had a lot of factory workers and auto workers who were laid off, and they were trying to re-skill for the job market and enter non-factory jobs. Some of them didn't even like know how to use a mouse. [At the same time] I was trying to avoid having them get scammed and stay secure. That was a big thing for me. [...] So I would teach, you know, doing things that you might not look at normally. I was teaching them the difference with domain names, secure networks, things like that. It was just a lot of digital illiteracy. And now smartphones being so ubiquitous, a lot more people have the internet, but it's still a problem, because people just don't know how to stay safe." (P11)

Ultimately, while our participants had a deep understanding of the communities they served, many felt constrained by their teaching contexts and isolated in their goal of teaching for privacy literacy. When presented with a hypothetical scenario of teaching without any of the constraints of their realities, educators shared a host of topics and activities they wished to present to their communities, including targeted sessions on encryption, combating harassment, and analyzing privacy policies, among others. For instance, without time and support constraints, P15 shared how they'd like to offer individual privacy audits (i.e., comprehensively reviewing all of an individual's current privacy and security practices) to patrons of their community library.

> "I mean, without like, any time or money constraints, I think being able to have the resources for somebody to individually come to the library—if there was the ability for somebody, especially in these small libraries, [...] to get a privacy audit. But those [libraries], you know, may not have time or staff to actually do the thing. And it may still feel intimidating to get started. And so I think being able [to] help give people the resources to, like, get started and just to come in and do a privacy audit, I think, is a really eye opening way of like, 'let's take a look at what you're doing,' right?" (P15)

Within our interview sessions, educators shared various desires, motivations, and challenges in improving learning outcomes for privacy literacy within their communities. Next, we discuss strategies for empowering educators, addressing the gaps between their

teaching desires and limitations, and ultimately supporting their resolve of achieving more widespread privacy literacy.

5 Discussion

Our study examined the pedagogical approaches and experiences of community-engaged educators in promoting privacy literacy. Through interviews with 21 educators across the U.S., our study provides a unique perspective on a highly valuable, yet understudied, context of privacy education. This work highlights the role of community-engaged educators in empowering their students to make informed decisions about their data. Our findings reveal that these educators prioritize critical thinking and personalization over rote memorization, emphasizing five core competencies essential to privacy literacy. However, despite their efforts, educators also face constraints that limit the reach of their programming. Through our findings, this study extends the conversation on privacy education and definitions of privacy literacy.

5.1 Expanding Definitions of Privacy Literacy

Our findings contribute to expanding our understanding of privacy literacy in multiple ways.

5.1.1 Emphasizing adaptability and decision-making. Our findings reveal that community-engaged educators view privacy literacy as a dynamic-process of critical thinking that enables individuals to make informed data decisions tailored to their personal contexts. This emphasis on adaptability and independent decision-making moves beyond rote memorization and instead aligns with the fluid nature of the digital world, where new technologies and privacy challenges are constantly unfolding.

5.1.2 Benefits of community-engaged education. The position of community-engaged educators is central to this effort. Our findings show that these individuals play a multi-faceted role, and are perceived by their students as both technical authorities and trusted community members. This dual role makes them particularly effective. Prior research shows that many individuals, especially those with lower income, less education, and older populations seek advice on these topics from personal, social connections rather than generic advice found online, in media, texts, or other resources [55, 56]. This positions community-engaged educators well to address the needs of diverse and often vulnerable communities in informal learning environments.

5.1.3 Integrating privacy, security, and online safety. Educators described an adaptable skill set grounded in five core competencies that form the foundation for privacy literacy: data fluency, account security, fraud detection, information vetting, and surveillance capitalism. These competencies address the community-driven needs highlighted by participants in our study and reflect how security, privacy, and online safety issues form interwoven threats for individuals. While participants recognized differences between privacy and security, they considered the combination of privacy, security, and online safety competencies crucial for developing privacy literacy.

5.1.4 Aligning privacy advice with community needs. Our findings further show differences between the topics prioritized by community educators and those emphasized in traditional cybersecurity guidance. For example, while prior literature has widely discussed the importance of cookies and cookie settings [30, 31], the educators in our study placed greater emphasis on issues with high potential for tangible harm to their students, such as financial fraud and scams affecting older adults and other groups, and devoted less attention to topics that were not central to their audiences' immediate needs, such as encryption or cookies.

This gap between community-driven priorities and expert-driven advice highlights an opportunity for fruitful collaboration between educators and experts to co-design more relevant privacy education frameworks that reflect community priorities. Realizing the potential of such co-designed frameworks requires addressing the resource, organizational, and policy supports that enable educators to implement them effectively, which we explore in the next section.

5.2 Needs and Support for Community Privacy Education

While the educational efforts of our participants provide tremendous value for their communities, educators also discussed several hurdles they faced in carrying out their trainings, such as time, organizational, and resource constraints, as well as broader structural and policy barriers. Building on our findings, we identify four areas where targeted support could enhance the effectiveness and reach of community privacy education.

5.2.1 Resource and organizational constraints. Educators faced persistent challenges in securing and maintaining the resources necessary for high-quality community-specific privacy education. Many struggled to access comprehensive standardized privacy materials, or felt overwhelmed by the sheer volume of privacy and security advice available online [59]. As a result, they often relied on personal knowledge, or organizational experience rather than on existing resources.

Some valuable resources, such as those from EFF, were unfamiliar or entirely unknown to some participants, highlighting challenges with discoverability even when high-quality resources exist. Educators also faced difficulties adapting materials quickly enough to address emerging privacy threats and evolving technologies, particularly given limited time, funding and staff support.

Low student interest in privacy-specific offerings presented additional barriers, especially when working with non-tech savvy individuals who faced competing priorities, such as financial insecurity. Under-resourced organizations often lacked the budget for marketing and outreach, making it difficult to attract participants. These constraints mirror broader patterns in digital literacy work, where educators must balance the ambition of tailored programming with practical limits of time, funding, and expertise [2].

5.2.2 Practical recommendations for supporting educators. To help overcome resource limitations and improve outcomes, community educators could benefit from sharing resources, strategies, and teaching materials through centralized platforms or peer networks, as peer support in volunteer settings has been shown to be effective

in amplifying efforts [33]. Modular, adaptable educational materials as they already exist in the broader digital literacy context [21, 35] could similarly offer an effective balance of consistency and flexibility for privacy literacy initiatives. Encouraging educators to leverage available resources (e.g., EFF materials) and fostering stronger connections between practitioners could further help address the identified gaps in accessibility and discoverability of privacy resources.

5.2.3 Policy and structural recommendations. Informal educational spaces, notably public libraries, can play a critical role in addressing digital inequities and advancing privacy literacy, particularly among marginalized communities [62]. Policy changes at local, state, and federal levels are thus essential to support these efforts, including increased funding and incentives for privacy educators and organizations [13, 44].

Additional financial support could help educators implement effective, personalized educational approaches more consistently, such as one-on-one consulting or hands-on training activities. Collaboration among government agencies, community organizations, research institutions, and educational institutions could help foster broader privacy literacy advancement ensuring that privacy education is recognized and prioritized as a key public service effort.

5.2.4 Directions for future research. Future studies could investigate the development and efficacy of a centralized repository of privacy education resources tailored to diverse communities and populations. Further research is needed to evaluate how modular resources can be effectively adopted and adapted to different contexts and community needs in practice. Moreover, exploring methods for facilitating effective collaboration between community educators and technical or pedagogical experts could address the identified gap between expert advice and educator-identified community needs. Finally, systematic studies assessing the impact of funding and policy interventions on community privacy educator outcomes could provide evidence-based insights to inform future structural support.

6 Conclusion

Our study expands on prior research working to define and operationalize the concept of privacy literacy [7, 32, 50, 72]. Through investigating the experiences of community-engaged educators whose work empowers their communities to become more privacy literate, we found that they believe privacy literacy is best represented as a conceptual process for informed decision making, centered around five core competencies that explicitly integrate privacy security, and online safety aspects. Our participants shared their working definitions of privacy literacy, the essential knowledge they believe is critical for achieving it, as well as strategies they employed within their ‘classrooms, which included various informal learning environments, to reach the diverse audiences they served. Given that privacy is deeply dependent on an individual’s sociocultural context [39, 45, 74], community-engaged privacy education appears to be a promising approach to foster privacy literacy. Our study contributes new insights on the understudied perspective of educators at the forefront of this effort, and helps to deepen our understanding of privacy literacy and respective priorities. We further present education and research implications to better support community-engaged educators, and ultimately the communities they serve, to broadly advance privacy literacy.

Acknowledgments

This research has been partially supported by the Defense Advanced Research Projects Agency (DARPA) under grant No. HR00112010010. Byron M. Lowens has been partially supported by a CRA/NSF CI Fellowship under grant No. 2030859. The content of the information does not necessarily reflect the position or the policy of the U.S. Government, and no official endorsement should be inferred. Approved for public release; distribution is unlimited.

References

[1] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2015. Privacy and human behavior in the age of information. *Science* 347, 6221 (2015), 509–514.
[2] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2020. Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology* 30, 4 (2020), 736–758.
[3] PA Adler. 1994. Observational techniques. *Handbook of qualitative research/Sage* (1994).
[4] Tanisha Afnan, Yixin Zou, Maryam Mustafa, Mustafa Naseem, and Florian Schaub. 2022. Aunties, strangers, and the {FBI}: Online privacy concerns and experiences of {Muslim-American} women. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. 387–406.
[5] Esma Aïmeur, Sabrine Amri, and Gilles Brassard. 2023. Fake news, disinformation and misinformation in social media: a review. *Social Network Analysis and Mining* 13, 1 (2023), 30.
[6] American Library Association et al. 2013. Digital literacy, libraries, and public policy: Report of the office for information technology policy’s digital literacy task force. *Retrieved January* 20 (2013), 2015.
[7] Miriam Bartsch and Tobias Dienlin. 2016. Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior* 56 (2016), 147–154.
[8] Ruha Benjamin. 2019. *Race after technology: Abolitionist tools for the new Jim code.* John Wiley & Sons.
[9] 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*. 610–622.
[10] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (2006), 77–101.
[11] Janet X Chen, Allison McDonald, Yixin Zou, Emily Tseng, Kevin A Roundy, Acar Tamersoy, Florian Schaub, Thomas Ristenpart, and Nicola Dell. 2022. Trauma-informed computing: Towards safer technology experiences for all. In *Proceedings of the 2022 CHI conference on human factors in computing systems*. 1–20.
[12] Danielle Keats Citron and Daniel J Solove. 2022. Privacy harms. *BUL Rev.* 102 (2022), 793.
[13] William Crumpler and James A Lewis. 2022. *Cybersecurity Workforce Gap*. JSTOR.
[14] Alaa Daffalla, Lucy Simko, Tadayoshi Kohno, and Alexandru G Bardas. 2021. Defensive technology use by political activists during the Sudanese revolution. In *2021 IEEE symposium on security and privacy (SP)*. IEEE, 372–390.
[15] Sauvik Das, Joanne Lo, Laura Dabbish, and Jason I Hong. 2018. Breaking! A typology of security and privacy news and how it’s shared. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–12.
[16] Laurien Desimpelaere, Liselot Hudders, and Dieneke Van de Sompel. 2020. Knowledge as a strategy for privacy protection: How a privacy literacy training affects children’s online disclosure behavior. *Computers in human behavior* 110 (2020), 106382.
[17] Serge Egelman, Julia Bernd, Gerald Friedland, and Dan Garcia. 2016. The teaching privacy curriculum. In *Proceedings of the 47th ACM technical symposium on computing science education*. 591–596.
[18] Stacy-Ann Elvy. 2018. Commodifying consumer data in the era of the internet of things. *BCL Rev.* 59 (2018), 423.
[19] Yoram Eshet. 2012. Thinking in the digital era: A revised model for digital literacy. *Issues in informing science and information technology* 9, 2 (2012), 267–276.
[20] HTTPS Everywhere. 2014. Electronic frontier foundation. *URL: https://www. eff. org/https-everywhere (visited on 31/07/2014)* (2014).
[21] Garry Falloon. 2020. From digital literacy to digital competence: the teacher digital competency (TDC) framework. *Educational technology research and development* 68, 5 (2020), 2449–2472.
[22] Daniel J Flynn, Brendan Nyhan, and Jason Reifler. 2017. The nature and origins of misperceptions: Understanding false and unsupported beliefs about politics.

Political psychology 38 (2017), 127–150.

[23] Anjuli Franz, Verena Zimmermann, Gregor Albrecht, Katrin Hartwig, Christian Reuter, Alexander Benlian, and Joachim Vogt. 2021. {SoK}: Still Plenty of Phish in the Sea—A Taxonomy of {User-Oriented} Phishing Interventions and Avenues for Future Research. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. 339–358.

[24] Ari B Friedman, Chris Pathmanabhan, Allen Glicksman, George Demiris, Anne R Cappola, and Matthew S McCoy. 2022. Addressing online health privacy risks for older adults: a perspective on ethical considerations and recommendations. *Gerontology and Geriatric Medicine* 8 (2022), 23337214221095705.

[25] Christine Geeng, Mike Harris, Elissa Redmiles, and Franziska Roesner. 2022. " Like Lesbians Walking the Perimeter": Experiences of {US}.{LGBTQ+} Folks With Online Security, Safety, and Privacy Advice. In *31st USENIX Security Symposium (USENIX Security 22)*. 305–322.

[26] 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*. 1–15.

[27] Said Gulyamov and Sherzod Raimberdiyev. 2023. Personal data protection as a tool to fight cyber corruption. *International Journal of Law and Policy* 1, 7 (2023), 1–35.

[28] 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*. 7057–7069.

[29] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. {"... No} one Can Hack My {Mind"}: Comparing Expert and {Non-Expert} Security Practices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. 327–346.

[30] Michael Kretschmer, Jan Pennekamp, and Klaus Wehrle. 2021. Cookie banners and privacy policies: Measuring the impact of the GDPR on the web. *ACM Transactions on the Web (TWEB)* 15, 4 (2021), 1–42.

[31] Oksana Kulyk, Peter Mayer, Melanie Volkamer, and Oliver Käfer. 2018. A concept and evaluation of usable and fine-grained privacy-friendly cookie settings interface. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, 1058–1063.

[32] Priya C Kumar, Mega Subramaniam, Jessica Vitak, Tamara L Clegg, and Marshini Chetty. 2020. Strengthening children's privacy literacy through contextual integrity. *Media and Communication* 8, 4 (2020), 175–184.

[33] Elizabeth M Lee and Jacob Harris. 2020. Counterspaces, Counterstructures: Low-Income, First-Generation, And Working-Class Students' Peer Support At Selective Colleges 1. In *Sociological forum*, Vol. 35. Wiley Online Library, 1135–1156.

[34] Ada Lerner, Helen Yuxun He, Anna Kawakami, Silvia Catherine Zeamer, and Roberto Hoyle. 2020. Privacy and activism in the transgender community. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–13.

[35] Heather Lotherington and Jennifer Jenson. 2011. Teaching multimodal and digital literacy in L2 settings: New literacies, new basics, new pedagogies. *Annual review of applied linguistics* 31 (2011), 226–246.

[36] Allan Martin. 2008. Digital literacy and the "digital society". *Digital literacies: Concepts, policies and practices* 30, 151 (2008), 1029–1055.

[37] 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*. 2189–2201.

[38] Allison McDonald, Catherine Barwulor, Michelle L Mazurek, Florian Schaub, and Elissa M Redmiles. 2021. " It's stressful having all these phones": Investigating Sex Workers' Safety Goals, Risks, and Practices Online. In *30th USENIX Security Symposium (USENIX Security 21)*. 375–392.

[39] 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*. 1–14.

[40] Joy McLeod, Leah Zhang-Kennedy, and Elizabeth Stobert. 2024. Comparing Teacher and Creator Perspectives on the Design of Cybersecurity and Privacy Educational Resources. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. 587–603.

[41] Collins W Munyendo, Yasemin Acar, and Adam J Aviv. 2022. "desperate times call for desperate measures": User concerns with mobile loan apps in kenya. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2304–2319.

[42] Collins W Munyendo, Yasemin Acar, and Adam J Aviv. 2023. " In Eighty Percent of the Cases, I Select the Password for Them": Security and Privacy Challenges, Advice, and Opportunities at Cybercafes in Kenya. In *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, 570–587.

[43] Sheza Naveed, Hamza Naveed, Mobin Javed, and Maryam Mustafa. 2022. " Ask this from the person who has private stuff": Privacy Perceptions, Behaviours and Beliefs Beyond WEIRD. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–17.

[44] William Newhouse, Stephanie Keith, Benjamin Scribner, and Gregory Witte. 2016. *NICE Cybersecurity Workforce Framework (NCWF): National Initiative for Cybersecurity Education*. Technical Report. National Institute of Standards and Technology.

[45] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash. L. Rev.* 79 (2004), 119.

[46] Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3). 2023. 2023 Internet Crime Report. https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf

[47] Kentrell Owens, Anita Alem, Franziska Roesner, and Tadayoshi Kohno. 2022. Electronic Monitoring Smartphone Apps: An Analysis of Risks from Technical,{Human-Centered}, and Legal Perspectives. In *31st USENIX Security Symposium (USENIX Security 22)*. 4077–4094.

[48] Kentrell Owens, Camille Cobb, and Lorrie Cranor. 2021. "You Gotta Watch What You Say": Surveillance of Communication with Incarcerated People. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–18.

[49] Yong Jin Park. 2013. Digital literacy and privacy behavior online. *Communication research* 40, 2 (2013), 215–236.

[50] Christine Prince, Nessrine Omrani, Adnane Maalaoui, Marina Dabic, and Sascha Kraus. 2021. Are we living in surveillance societies and is privacy an illusion? An empirical study on privacy literacy and privacy concerns. *IEEE Transactions on Engineering Management* 70, 10 (2021), 3553–3570.

[51] Emilee Rader and Rick Wash. 2015. Identifying patterns in informal sources of security information. *Journal of Cybersecurity* 1, 1 (2015), 121–144.

[52] Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*. 1–17.

[53] Lubna Razaq and Sucheta Ghoshal. 2024. What to the Muslim is Internet search: Digital Borders as Barriers to Information. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–17.

[54] Pritika Reddy, Bibhya Sharma, and Kaylash Chaudhary. 2020. Digital literacy: A review of literature. *International Journal of Technoethics (IJT)* 11, 2 (2020), 65–94.

[55] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. 2016. How i learned to be secure: a census-representative survey of security advice sources and behavior. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. 666–677.

[56] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. 2017. Where is the digital divide? a survey of security, privacy, and socioeconomics. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 931–936.

[57] Elissa M Redmiles, Amelia R Malone, and Michelle L Mazurek. 2016. I think they're trying to tell me something: Advice sources and selection for digital security. In *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, 272–288.

[58] Elissa M Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L Mazurek. 2020. A comprehensive quality evaluation of security and privacy advice on the web. In *29th USENIX Security Symposium (USENIX Security 20)*. 89–108.

[59] Robert W Reeder, Iulia Ion, and Sunny Consolvo. 2017. 152 simple steps to stay safe online: Security advice for non-tech-savvy users. *IEEE Security & Privacy* 15, 5 (2017), 55–64.

[60] Rahime Belen Sağlam, Vincent Miller, and Virginia NL Franqueira. 2023. A systematic literature review on cyber security education for children. *IEEE Transactions on Education* 66, 3 (2023), 274–286.

[61] Nithya Sambasivan, Nova Ahmed, Amna Batool, Elie Bursztein, Elizabeth Churchill, Laura Sanely Gaytan-Lugo, Tara Matthews, David Nemar, Kurt Thomas, and Sunny Consolvo. 2019. Toward gender-equitable privacy and security in south asia. *IEEE Security & Privacy* 17, 4 (2019), 71–77.

[62] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. 2018. " Privacy is not for me, it's for those rich women": Performative Privacy Practices on Mobile Phones by Women in South Asia. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. 127–142.

[63] 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. *Proceedings of the ACM on Human-computer Interaction* 2, CSCW (2018), 1–27.

[64] Erica Shusas, Patrick Skeba, Eric PS Baumer, and Andrea Forte. 2023. Accounting for Privacy Pluralism: Lessons and Strategies from Community-Based Privacy Groups. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–12.

[65] Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. 2018. Computer security and privacy for refugees in the United States. In *2018 IEEE symposium on security and privacy (SP)*. IEEE, 409–423.

[66] Manya Sleeper, Tara Matthews, Kathleen O'Leary, Anna Turner, Jill Palzkill Woelfer, Martin Shelton, Andrew Oplinger, Andreas Schou, and Sunny Consolvo. 2019. Tough times at transitional homeless shelters: Considering the impact of financial insecurity on digital security and privacy. In *Proceedings of the 2019 CHI*

Conference on Human Factors in Computing Systems. 1–12.
[67] Daniel J Solove. 2005. A taxonomy of privacy. *U. Pa. l. Rev.* 154 (2005), 477.
[68] Valdemar Švábenskỳ, Jan Vykopal, and Pavel Čeleda. 2020. What are cybersecurity education papers about? a systematic literature review of sigcse and iticse conferences. In *Proceedings of the 51st ACM technical symposium on computer science education*. 2–8.
[69] Mindy Tran, Collins W Munyendo, Harshini Sri Ramulu, Rachel Gonzalez Rodriguez, Luisa Ball Schnell, Cora Sula, Lucy Simko, and Yasemin Acar. 2024. Security, Privacy, and Data-sharing Trade-offs When Moving to the United States: Insights from a Qualitative Study. In *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE, 617–634.
[70] Daricia Wilkinson and Bart Knijnenburg. 2022. Many islands, many problems: An empirical examination of online safety behaviors in the caribbean. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–25.
[71] 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*. 51–69.
[72] Christina L Wissinger. 2017. Privacy literacy: From theory to practice. *Communications in Information Literacy* 11, 2 (2017), 378–389.
[73] Michael Zimmer and Bonnie Tijerina. 2018. Library values & privacy in our national digital strategies: Field guides, convenings, and conversations. *Milwaukee, WI: Center for Information Policy Research. https://cpb-us-w2. wpmucdn. com/people. uwm. edu/dist/b/524/files/2018/08/LibraryValuesAndPrivacy_Report-28qqhtp. pdf* (2018).
[74] Yixin Zou, Kaiwen Sun, Tanisha Afnan, Ruba Abu-Salma, Robin Brewer, and Florian Schaub. 2024. Cross-Contextual Examination of Older Adults' Privacy Concerns, Behaviors, and Vulnerabilities. *Privacy-Enhancing Technologies (PoPETs)* (2024).
[75] Shoshana Zuboff. 2023. The age of surveillance capitalism. In *Social theory re-wired*. Routledge, 203–213.

A Study Materials

Relevant study materials are available in our OSF repository: https://osf.io/g3p7c/