Leveraging Funds of Knowledge to Manage Privacy Practices in Families

Mega Subramaniam, Priya Kumar, Shandra Morehouse, Yuting Liao, and Jessica Vitak
College of Information Studies, University of Maryland
College Park, MD, United States of America
{mmsubram, pkumar12, shandra, yliao598, jvitak}@umd.edu

ABSTRACT

Information and communication technologies play a critical role at home, school, and work for people of all ages. At the same time, use of these technologies can present challenges to privacy and security. In this study, we apply the concept of funds of knowledge to understand how families develop knowledge and skills around using technology and protecting personal information. Funds of knowledge explains how people gain knowledge and highlights how learning happens in a variety of environments beyond the classroom. Through interviews with 52 families living in economically disadvantaged communities in the United States, we develop a typology of privacy funds of knowledge in families. We also explore how privacy funds of knowledge inform families' privacy practices. We conclude the paper by identifying how these findings inform the development of resources for families to further enhance their digital practices.

KEYWORDS

Privacy; security; digital youth; digital literacies; funds of knowledge; youth information behavior; family learning

ASIS&T THESAURUS

Information Behavior; Communities; United States

INTRODUCTION

Families interact with a variety of information and communication technologies at work, home, and school. Smartphones and tablets are common and are increasingly used in public school systems as a part of formal education, while "smart" technologies like digital voice assistants and location-tracking devices are becoming more affordable for homes and more common in public spaces. Yet use of these technologies presents challenges to data privacy and security. How do people learn how to address these risks?

In addition to more formal educational settings, people turn to a variety of sources to develop digital competence, including through their interactions with family, friends, and their wider community. A prominent concept for describing how young people gain and share knowledge from sources beyond formal education environments is *funds of knowledge* (Moll & Greenberg, 1990). Funds of knowledge recognizes that children, families, and communities gain valuable knowledge from life experience that can form the basis for—and supplement—formal learning practices.

In this paper, we investigate how families draw on funds of knowledge to learn about privacy and enhance their privacy practices. Specifically, we address the following research questions:

RQ1: What knowledge sources shape the privacy funds of knowledge in families?

RQ2: How do personal experiences contribute to the development of privacy funds of knowledge in families?

To answer these questions, we examine data we collected from 52 families (54 adults and 23 children) who live or work in the state of Maryland (USA). Our findings are part of a larger project funded by the Institute of Museum and Library Services (IMLS), with data collected in partnership with our state's division of library services. In 2017, we partnered with four libraries across the state and a non-profit organization that works with Latinx[1] families to interview families from economically disadvantaged communities. We talked about their technology practices and challenges or barriers they faced when using technology. Specifically, we wanted to explore the privacy and security risks these families faced when using digital technology. Our project's goal is to develop resources to help families enhance their privacy practices and make better-informed decisions about their online data. We are also creating resources to help library staff address privacy and security concerns that may emerge when they assist patrons with online transactions that involve sensitive information. In this paper, we offer a typology of privacy funds of knowledge that low-income families draw on to inform their privacy practices. Our typology presents an alternative to the concept of privacy literacy and highlights

82nd Annual Meeting of the Association for Information Science & Technology | Melbourne, Australia | 19 – 23 October, 2019

[1] This is a gender-neutral term referring to people from Latin American cultures.

the varied avenues through which knowledge acquisition happens across and within social networks.

RELATED FRAMEWORKS

In this section, we discuss the concept of funds of knowledge—its origin, the social contexts and networks that constitute funds of knowledge, and the importance of tapping into funds of knowledge for learning among underserved young adults. We then review the concept of privacy literacy and highlight how people and families develop related knowledge and skills.

Funds of Knowledge for Family Learning

Funds of knowledge, a concept from education literature, refers to the idea that children bring a diverse background of knowledge gained from their family and community into the classroom. Vélez-Ibáñez & Greenberg (1992, p. 313) define funds of knowledge as "the strategic and cultural resources...that households contain." Funds of knowledge come from a variety of social contexts and networks in a child's life. These include the child's own knowledge, the child's parents and relatives, other children and their family members, teachers' networks, school staff, and other community members (Moll & Greenberg, 1990). Moje et al. (2004) simplify this into four categories of funds of knowledge: family, community, peers, and pop culture.

In addition to gaining funds of knowledge through individual experiences (Moll & Greenberg, 1990), families access funds of knowledge from their immediate household, extended family, and friends. These social networks can "facilitate the development and exchange of resources, including knowledge, skills, and labor" (Moll, Amanti, Neff, & Gonzalez, 1992, p. 133). In their work with Mexican-American families in the Southwestern U.S., Vélez-Ibáñez & Greenberg (1992) found that a family's social network provides assistance and information regarding housing, jobs, and government services. Family social events (e.g., birthdays, weddings) also contribute to funds of knowledge (Barton & Tan, 2009; Vélez-Ibáñez & Greenberg, 1992).

Beyond their social networks, families also turn to community funds of knowledge, which can include formal groups (e.g., government agencies, labor unions, schools) that provide information and assistance (Vélez-Ibáñez & Greenberg, 1992). Community groups and organizations like churches, libraries, and after-school programs are a source of ethnic identity within communities; this ethnic identity plays a major role in developing an individual's funds of knowledge (Moje et al., 2004).

Students also acquire funds of knowledge from their peers. Moje et al. (2004) show how "hanging out" with peers in informal settings (i.e., spaces not mediated by adults), provides opportunities for students to teach each other skills or provide assistance (e.g., helping English language learners with their homework). Young people spend time online together, looking up their interests and refining their search strategies—skills that are also useful in classroom settings. Additionally, peers learn culture from one another, including popular music, fashion, and vernacular (Moje et al., 2004).

Connecting Funds of Knowledge and Learning

People need to make connections between the various types of funds of knowledge they encounter to actually learn a concept. Vygotsky's (1978) theory on the zone of proximal development (ZPD) identifies the space between what individuals can do with help and what they can do without help. Drawing on funds of knowledge can help someone move from needing support to fully understanding a concept (Moll & Greenberg, 1990).

Teachers play an important role connecting a student's funds of knowledge with classroom learning objectives (Kajamaa, Kumpulainen, & Rajala, 2018). Moll et al. (1992, p. 137) refer to teachers as "the ultimate bridge" to the student's world, their funds of knowledge, and the learning in the classroom. By allowing students to access their own funds of knowledge for learning, teachers put learning in students' hands, taking the role of facilitator rather than expert authority (Barton & Tan, 2009).

Family members make connections between funds of knowledge and learning as they interact with each other (Moll et al., 1992). Children also make these connections by asking family members questions, observing activities, and practicing learned behavior through play (Vélez-Ibáñez & Greenberg, 1992).

Leveraging Funds of Knowledge in Teaching and Learning with Underserved Families

Moll et al. (1992, p. 20) explain that classroom and research agendas usually assume that minority students come from "socially and intellectually limiting family environments, or that these students lack ability, or there is something wrong with their thinking or their values, especially in comparison to their wealthier peers." But, "funds of knowledge is an antithesis to this approach" (Mills, 2019, p. 7). Children, their families, and communities are assumed to be competent and possess valuable knowledge gained from life experience that forms the basis for education. Using funds of knowledge in the classroom for instruction is a way to legitimize and value students' out-of-school experiences in their home or community (Kajamaa et al., 2018).

Mills (2019) examines funds of knowledge in the context of science education. She identifies four settings for funds of knowledge—home, neighborhood, school, and after school. She explores how digital technology and other learning environments can supplement scientific funds of knowledge, particularly in underserved communities. Other researchers have explored how underserved students can draw on funds of knowledge to bring their cultural experiences into the classroom (Barton & Tan, 2009; Chen, Carger, & Smith, 2017).

Most of this work focuses on bringing funds of knowledge into formal education settings (Chen et al., 2017) or using it to improve school curricula (Mills, 2019). While studies on funds of knowledge have examined families as the unit of analysis, they typically focus on children learning from family members rather than on the different funds of knowledge each family member contributes to collective family learning. To the best of our knowledge, our study represents the first that considers how individuals integrate privacy-related funds of knowledge within their families and is not focused directly on school-based curricula.

Privacy Literacy

Privacy literacy refers to an individual's "level of understanding and awareness of how information is tracked and used in online environments, and how that information can retain or lose its private nature" (Givens, 2015, p. 58). Trepte et al. (2015, p. 339) further specify that privacy literacy encompasses "factual or declarative ('knowing that') and procedural ('knowing how') knowledge." In other words, it is not enough for someone to know *that* information is tracked online; they should also know *how* (if at all) they can limit such tracking.

Survey research highlights areas where privacy knowledge is low. For example, Americans consistently misunderstand the function of a privacy policy, with around half inaccurately believing that the existence of a policy means that companies do not share personal information with others (Turow et al., 2014). Most American internet users also lack understanding of relevant cybersecurity topics, such as encryption, private browsing, or VPNs (Smith, 2017). And while most American internet users recognize that companies track their online activities (Turow et al., 2014), many do not know that companies can legally sell consumer data to others or charge different prices based on such data (Turow, Hennessey, & Draper, 2015).

Researchers have also examined the factors that inform privacy literacy and the outcomes to which it contributes. People who spend more time on social media and who change their privacy settings frequently are more likely to have higher privacy literacy (Bartsch & Dienlin, 2016). Privacy literacy does not affect people's information sharing behaviors (Baruh, Secinti, & Cemalcilar, 2017), but those with higher privacy literacy and technical familiarity are more likely to take steps to control the flow of their information online (Bartsch & Dienlin, 2016; Park, 2013). Yet Park (2013) noted that overall levels of privacy literacy have remained low—even as access to technology increased—suggesting that the divide in digital skills encompasses privacy.

Indeed, recent research questions how digital literacy influences privacy behaviors. Researchers have observed that people increasingly approach online privacy with a sense of resignation (Turow et al., 2015). Hagendorff (2018) critiques the concept of privacy literacy, arguing that since people who have higher privacy literacy tend to have higher incomes and education, gaps in privacy literacy will persist while income and education remain unequally distributed.

Developing Privacy Knowledge

Privacy literacy research has explored *what* people know about online data flows, but more work is needed on *how* people develop this knowledge. In a representative survey of American adults, Redmiles, Kross, and Mazurek (2017) found that people primarily learn security-related information (e.g., passwords, antivirus programs, software updates, two-factor authentication) from media as well as family and friends. People also learn from their own negative experiences, from companies such as internet service providers or banks, and through their workplaces. They accept advice largely when they trust the source and reject advice that is inconvenient or contains too much marketing material (Redmiles et al., 2017). Different types of information also serve distinct purposes. Rader and Wash (2015) suggest that personal stories can help people care about security while expert advice can tell people how best to protect themselves online.

Indeed, Wash and Rader (2011) argue that people's security knowledge may matter less than their beliefs about online risk and how to mitigate it. They argue that security researchers should focus on getting people to make the right security decision rather than ensuring they have the right security knowledge. This approach makes sense in the security realm, where potential actions are less value-laden. For example, while people may find two-factor authentication confusing or inconvenient, there is little question that it makes a login process more secure. Privacy-related decisions, such as the disclosure of information, are often less clear cut and more context-dependent.

People's privacy beliefs and attitudes are informed by various sources, beginning with their families. As children spend more time in community institutions such as school, they gain awareness of group and social norms regarding interaction and information management (Petronio, 2002). And as digital technologies have embedded into families' everyday lives, extensive research has explored how children and families navigate online risks (e.g., Livingstone, Haddon, & Görzig, 2012). Parents of teenagers tend to more actively help their children navigate online privacy concerns (Wisniewski, Jia, Xu, Rosson, & Carroll, 2015), while parents of younger children may believe their children do not need such guidance until they are older (Kumar et al., 2017). Indeed, parents of younger children may be missing an opportunity to meet children in their zone of proximal development and scaffold their development of online privacy management skills (Kumar et al., 2017). In addition to the home, schools and libraries are well-positioned to help children (and adults) develop privacy knowledge and skills (Agosto & Abbas, 2016; Givens, 2015; Kumar, Chetty, Clegg, & Vitak, 2019;

Wissinger, 2017). Our work identifies the different funds of knowledge on which such efforts can build.

METHODS

Recruitment

At the start of the project, we identified four partner library branches in economically disadvantaged areas of the state. Table 1 includes general information about the partner libraries and the communities they serve, including their general location, unemployment rate, and poverty rate. Library branch managers and staff helped us recruit participants. We created fliers and shared details of the study with library staff, and they identified patrons who fit our recruitment criteria. We also partnered with a local non-profit organization that works primarily with disadvantaged Latinx families who are immigrants and speak English as a second language. We relied heavily on partners' knowledge of the local community and library patrons to help us identify likely participants. Going through these organizations to recruit families, rather than trying to recruit directly, helped us establish trust and rapport with community members and assuaged potential concerns about the research.

Branch	Location	Unemployment Rate in the area	Poverty Rate
A	Rural	14%	28%
B	Urban	12%	24%
C	Urban	17%	20%
D	Rural	11%	20%

Table 1. Descriptive details for partner library branches

Data Collection

From March—May 2017, we conducted face-to-face interviews with 46 families at the four partner libraries. In June 2017, we interviewed six additional families at a public center run by our nonprofit partner. In total, we spoke with 54 adults and 23 children from 52 families (13 identifying as Latinx). Our interviews lasted 25—75 minutes. We encouraged multiple family members to attend so we could obtain a variety of perspectives. When children were present, we asked them specific questions about their technology use at home and school and whether they had learned about online safety or security at school. Each family received US$75 cash as compensation.

Data Analysis

We had the interviews transcribed and imported the transcripts into the qualitative analysis software Dedoose. We created an initial codebook based on the existing interview protocol and broader research goals, and each member of the research team separately coded one interview. We then discussed the coding process and refined the codebook. We repeated this process with a second interview and finalized the codebook. Our final codebook included 24 codes regarding adults' and children's attitudes and behaviors related to privacy/security. Each interview transcript went through two rounds of coding. In the first round, a team member coded the transcript, and in the second round, a different team member reviewed the coding decisions. The team met and resolved coding differences through discussion (Lincoln & Guba, 1985).

To address the current study's research questions, we focus our analysis on six codes covering children's technology use, technology literacy, sources of technology knowledge, and privacy behaviors, as well as parents' technology oversight practices and privacy behaviors. Given that our primary project goal is to create privacy resources families can use together and/or individually, we conducted another round of analysis on these six codes to identify how and from where children and adults bring funds of knowledge to manage privacy online. Researchers who have studied children's funds of knowledge in the educational space have devised typologies to categorize the sources of funds of knowledge (e.g., community, culture, family). However, none of these existing typologies have categorized funds of knowledge for privacy-related learning. Using the lens of funds of knowledge, we further analyzed the excerpts from these six codes closely for evidence of sources and categories of privacy funds of knowledge that families draw from, including personal experiences that shape privacy practices. Additionally, wherever possible, we also highlight less-protective privacy practices that families obtain through funds of knowledge, which will inform the privacy-related resources we create for families.

When reporting findings, we use alphanumeric identifiers to indicate where the interview was conducted and whether the participant was an adult or child. The alphabet before participant number refers to the library where we interviewed them (see Table 1). Latinx participants recruited from the local non-profit are labeled as "LN". The "-A" or "-C" after the identifier indicates whether the speaker was an adult or child, respectively.

FINDINGS

RQ1: What knowledge sources shape the privacy funds of knowledge in families?

Privacy Funds of Knowledge Through Formal and Informal Learning Settings

Formal schooling was the most salient context from which participants drew privacy knowledge, including both children's current experiences and adults' previous experiences. Children (and some adults) gained privacy knowledge in classes on computers, technology, financial literacy, and media. These included lessons on internet safety and instructions and/or strategies for protecting personal information online, such as creating strong passwords, being mindful of pop-ups, clearing caches and browsing history after using public computers, and using third-party services to monitor suspicious activities on one's accounts. For example, Participant A15-C said, "*They [the school] said do not ever put your personal information…they said not to click 'accept' to anything that pops up, to let us know about it before you do anything for any pop-ups.*" Likewise, Participant A3-A took a financial literacy class and learned about using third-party services that will *"send me alerts...anything looks suspicious...So how I have my (bank) account set up now, where nobody can take anything out of my account without ... being authorized by me first…"*

School lessons often focused on creating strong passwords—"*They [school] taught...how to type in eight to 12-digit passwords*" (B15-C)—and safeguarding them—"*They do tell everyone to sign off their email when you're done using the computer because that's been an issue sometimes if people are logged in with their email and somebody can go inside their email and send out emails pretending to be that person...*" (C13-C). While this is encouraging, some parents also said their children receive pre-set passwords from the school systems that use their names and/or birthdates. In some cases, these children cannot change the password and use the same password for other systems. One parent (C6-A), observed how this affected her child's privacy practices: *"...Because you use your birthday for everything. So, we know, your sister and I know you use your birthday for everything...What about creating different codes that only you would know?*" The child confirmed that her school had not taught her anything about *why* or *how* to do that.

Parents said they obtained privacy-related knowledge through their children's school lessons. For example, Participant A5-A said, *"...my 11-year-old, he feels pretty comfortable because he knows more about how to use some of the stuff, than me. He knows more sites because they talk about it a lot in school. That's where I learn a lot of my information. Whatever he learns at school, that's where I find stuff out.*" These exchanges highlight how privacy-related information children obtain in school can contribute and transfer to become family funds of knowledge.

Beyond school, some parents we interviewed received on-the-job-training and attended short or semester-long courses in colleges. These ranged from basic instructions on how to use the computer and the Internet to more specific lessons on topics such as animation or creating and sharing movies. These courses involved brief conversations about privacy practices, such as protecting personal information when completing tasks like sharing videos online. Our participants also described informal training on privacy in the form of one-hour classes or tutorials at the library or short discussions on internet safety during an English-language-learning class at a community center.

Developing Privacy Funds of Knowledge Through Family Interactions

Family members learn about privacy-related concepts and practices by sharing experiences with each other. These experiences and knowledge can be transferred from a child to a parent, from a parent to a child, between siblings, and can come from extended family members. We observed each of these in our analysis. We include any risky online practices participants discussed to highlight that such transfers that can be enriching or confusing.

Privacy Knowledge Shared from Child to Parent. Children assist parents in typical day-to-day practices such as finding information online, navigating social media, and completing essential transactions (e.g., shopping, submitting job applications). Regarding privacy, we found children imparting their knowledge about what features suggest trustworthiness on a website (i.e., lock icon next to a webpage URL), how to adjust social media settings (i.e., make a profile private), and how to configure phone settings (i.e., activating "Find my iPhone").

Privacy Knowledge Shared from Parent to Child. We found many instances where children follow parents' guidance. This included advice regarding tasks such as shopping from a trusted site. Participant A6-C said, "*...my mom does a lot of online stuff so I learned from her...I think she might do one clothing store that she really trusts. I even heard her say she hasn't had any problems with it.*" Parents also gave advice more directly related to safety and security. Participant B18-C, whose mother lived outside the U.S., said, "*...my mom told me, since she lives in my country [of origin], 'you have to be very careful with what you do,' not so much because of my safety here but rather for their [family] safety over there [in the child's country of origin]. Then I went through my friends and I started, not deleting them [unfriending], but putting them on restricted access. Out of all the friends I have, it's just a few who can see my things. The rest are there, but they can't see it. It's a safety measure because of the violence in our countries."*

Privacy Knowledge Shared Between Siblings. Children said they encountered websites that were not trustworthy and messages that could have been phishing attempts. They also helped—or were helped by—siblings in navigating difficult situations. Participant C5-C said his sister helped him avoid risk when responding to online prompts: "*My sister said, 'Don't. Just let me look at it first,' because she said sometimes it may appear to be secure like the actual site of Microsoft, but it might not be.*" He also said his older brother checked on him to see if he is *"downloading something that I should not."*

Privacy Knowledge Shared Via Extended Family. Participants said that extended family members who experienced privacy violations warned relatives by sharing their stories. Participant A15-C said her uncle's debit card number was stolen and "*they stole his money out of his bank account. It was for the kids' Christmas presents and they stole his money. That's why I don't trust nothing on the internet.*" Relatives also shared other useful information. For example, participant D3-A said her cousin recommended an internet service provider that offered web filtering services that aligned with her values. "*I had to give up AOL because, I mean, it was just inappropriate spam coming in. I didn't like that, so I went to a Christian internet provider and that turned that [spam] down about 90%.*"

Friends as a Source of Privacy Funds of Knowledge

Friends' experiences also influence people's privacy practices. Participant B19-A wanted to purchase handbags from Facebook ads but explained why she refrained: "*They sell $50 or something but this is fake...My friends told me this is fake bags.*" Participants also described instances when they hesitated because of privacy concerns and then were convinced by their friends to complete online transactions. Participant LN2-A said, "*This thing of sharing links is brand new to me and I'm still weirded out because I gave my address so that...just being able to do online jobs like they tell you, 'Oh, try to do this. Work at home. You just need the internet.' I don't trust those sites. She [my friend] did it and she said she got a check and we've known each other for 12 years so...okay, let me give it a try...Then when I started seeing the visits and the numbers and the numbers go up and the numbers go up every time you refresh the page, it'd be like, okay maybe. She's like, 'I wasn't very skeptical like you, but once I actually received a check with the amount that it showed on the computer and not a penny less, not a penny more, then I believed them.' I was like, wow. She said she made $800 in a month.*"

Trusting Sources Deemed "Experts" Help Develop Privacy Funds of Knowledge

Participants described accepting information from individuals with affiliations that suggested they were trustworthy or reliable. Participant LN5-A said she looks for the lock icon next to URLs because "*the girl from the bank told my husband about it...be sure to check it whenever he wanted to purchase something.*" Some interviewees said they ask librarians questions when they are completing online tasks in libraries *"...because if anything come up that's not right, they'll be notified. So, if I'm at home, on my own server I wouldn't even know. They [libraries] have all the right tools*" (A3-A). When participants had privacy questions, they often described asking someone who knows about the topic (without specifying who the "someone" was), hearing stories about negative experiences people had with certain websites (without specifying who the "people" were), and reading reviews for online services before engaging in online transactions to avoid being cheated or scammed.

Participants also described accepting information from well-established or popular organizations. They often referred to practices of larger companies as hallmarks of safe practices for dealing with sensitive information. Participant A4-A said, "*I know big businesses back up all their files and everything on the cloud. So, I guess it's safe. I'm sure all the big companies wouldn't put to cloud if it was not safe.*" Participants considered shopping sites such as Amazon and Etsy "legit organizations" because many people use them. Participant D1-A said, *"I'll buy off of Amazon, but...I wouldn't feel comfortable buying off of some platform I've never heard of or anything like that."* On the other hand, our participants did not trust Facebook the way they did Amazon. For example, one participant (LN6-A) consciously decided not to use the site in a family emergency*: "...a year ago one of my nieces went missing while she was on her way here [U.S.] from El Salvador. In order to keep the smuggler from realizing that we were… looking for her, it was better to go to the center [a non-profit that helps immigrants and refugees] to get help…I know that I could have posted it on Facebook… [but] I seek help another way."* She was concerned that posting information on Facebook may have tipped off the smugglers and put her niece in greater danger.

RQ2: How do personal experiences contribute to the development of privacy funds of knowledge in families?

When we asked participants how they knew about a given privacy-related practice, the most common response was, as Participant C12-C put it, "*I figured it out on my own.*" Personal experiences (in addition to the sources described above) are also a category of funds of knowledge (Moll & Greenberg, 1990).

Personal Encounters With Privacy Issues

Echoing Redmiles et al. (2017), our participants described how negative experiences led them to engage in protective behaviors. For example, Participant B5-A said, "*I had a strange guy come and knock on my door one time...This old white man...It was scary, and I shut the door real quick when I didn't know who it was...He tracked me on Facebook 'cause when I took a picture of me and my kids...posted it, it showed where I live, where I took the picture, the location. Everything... And when that guy comes to my house, I went on my Facebook and I turned the location off. 'Cause it was on. And then I turned the location off on my phone too."* Many of our adult participants said they avoided online banking (unless it was completely necessary) because they worried about their bank account information being compromised. Others limited important online transactions to a single computer at home because they feared getting hacked, or they purchased third-party identity theft protection because their social security or credit card numbers had been stolen and used in the past. Many were wary of pop-ups and ads that took them to websites that asked for personally identifiable information because of past experiences losing control of their computers to hackers. Some did not respond to messages promising instant cash because they learned this was a scam.

Conversely, positive experiences reinforced participants' digital practices. Participant A3-A used Indeed.com for her job applications, and she said, "*...I've been using that for years and I feel a little bit more secure with that.*" In addition to using services without any breaches or problems, many adults we interviewed looked for information before transacting with a company. Before buying something from a specific website, Participant A13-A did *"...a lot of research, pulling up a lot of websites, understanding where they're manufacturing it from. I've looked at them for some years, before I even purchased something from them. So, the consistency of their website, calling them up, and how their customer service is...*"

Personal Encounters with System-Programmed Privacy Measures

Some adults we interviewed relied on past experiences with their bank to flag questionable expenses in their account, and therefore protect them from being responsible for any purchases made that they had not authorized. Participant D1-A said, "*I've tried to buy things before from Etsy and it was going to New York state, and [my husband's] bank even flagged purchases coming from New York because at that time there had been a lot of, I guess, issues. So, it has flagged things before.*" She further explained her complete comfort with her bank, saying, *"...we've gone to go pay gas and you're at the pump and something's wrong and we'll get a call from the bank like, 'You've had this many charges today, is this you?' Or we'll get text messages and stuff. So, I feel comfortable [with] all those security measures on there...*"

Participants described similar experiences with other companies. Participant D7-A said she had not experienced identity theft or hacking but had received related warnings: "*Either I think we've gotten warnings that people have attempted or like they've attempted to access the Facebook account, and I think maybe it was the email or banking account—I forget which it was—but we got a warning from the company saying change your password, this was attempted to be cracked.*" Some participants said websites prompted them to change their passwords every three months, which got them into the habit of changing their passwords for every website they interact with. Some adults we interviewed described experiences receiving authentication codes, creating security questions, and interacting with Captchas. They considered these to be signals that websites protect their personal information and looked for them when interacting with new websites.

Participants paid attention to website prompts when setting up accounts, taking note of alerts about weak, medium, and strong passwords or alerts about logging into public WiFi. Participant LN2 said, "*to get to the McDonald's WiFi, it used to not let me go through and get it because they said it was not a trusted site.*" Participants also relied on online platforms to protect their privacy. Participant D2 said, "*I leave a lot of the security up to the Google.*" Similarly, participant LN3-A appreciated Google services that monitor for hacking and notify her through e-mails that say, "*You accessed your email on a certain computer, that was located at a certain place, let us know if that was you.*"

We summarize the typology of funds of knowledge that we found through our study in Table 2.

DISCUSSION

Through our analysis of interviews with 52 families, this paper presents a typology of funds of knowledge related to digital privacy. Below, we explain how our findings extend the funds of knowledge framework and inform the potential form, process, and content of the privacy resources that we will develop for economically disadvantaged families—and the libraries/librarians that serve them.

Funds of Knowledge	**Examples of sources of Funds of Knowledge**
Formal & Informal Learning Experiences	School and educational lessons (e.g., computer/technology classes, financial literacy training), on the job training, short and semester-long college courses, classes and tutorials at libraries, classes at a community center
Family Members	Learning from child, parent, sibling, extended family member
Friends	Friends' experiences, friends influence on privacy behavior
Sources deemed as Privacy "Expert"	*Individuals*: bank employees, librarians, "someone" (undefined), reviewers for services and websites *Organizations*: "big companies", "legit" organizations, Amazon, PayPal
Own Experience	Experiences with privacy issues, Experiences with system-programmed privacy measures

Table 2. Typology of funds of knowledge of digital privacy

Expanding Funds of Knowledge Framework to Privacy

Researchers have employed Moje et al.'s (2004) four categories of funds of knowledge—family, community, peers, and pop culture—in the context of science and language learning. We extend some of these categories to identify funds of knowledge related to privacy. While previous literature points to parents as sources of funds of knowledge for children (Moll & Greenberg, 1990), our research reveals that the flow of privacy knowledge can also move from children to parents, among siblings, and also across extended family members (e.g., cousins, uncles, aunts). Additionally, we highlight that while knowledge is shared within families, individual members also bring privacy-related knowledge gained from their own networks of peers and communities (RQ1) and through their own experiences (RQ2). A rich amalgamation of privacy knowledge flows among family members and forms privacy funds of knowledge within the family.

When it comes to privacy, community funds of knowledge go beyond schools and community centers to encompass workplaces and people or organizations deemed as "experts." Echoing Redmiles et al. (2017), the "someone" who supplies privacy tips and practices includes individuals who work in trusted organizations such as libraries; large companies such as Amazon and Etsy, banks, and internet service providers; and websites that provide visible signals that they protect the safety of their users. Particularly interesting are references to specific companies as sources of trusted funds of knowledge (e.g., trusting Amazon and Etsy, not trusting Facebook). This suggests possible influences of funds of knowledge from peers (family friends) and popular culture (media and television). The emergence of librarians as trusted sources of privacy funds of knowledge is particularly important to the growing literature that supports libraries as hubs for low-socioeconomic individuals to access support when completing essential tasks such as applying for housing, food assistance, etc. (Thompson, Jaeger, Taylor, Subramaniam, & Bertot, 2014; Vitak, Liao, Kumar, & Subramaniam, 2018a). This suggests an important opportunity for libraries and librarians to consider new ways to support the growth and development of their patrons' privacy skills.

For children, school and formal education environments seem to be the most prominent "community" source of privacy funds of knowledge. While previous research has mostly studied out-of-school experiences with the goal of enhancing in-school learning, our findings reveal the reverse, where knowledge gained in school enhanced everyday privacy practices. It is imperative to consider school as a strong source of "community" funds of knowledge in future endeavors to facilitate learning of emerging digital literacies. Echoing Kumar et al. (2019), we argue that school systems should consider incorporating privacy-specific lessons into their curricula, since our findings suggest young adults are referencing such learning in their everyday practices.

Individuals' negative and positive experiences with technology inform their privacy perceptions and practices (Redmiles et al., 2017). Our finding that many participants said they developed privacy knowledge on their own aligns with previous education literature (Barton & Tan, 2009; Moll & Greenberg, 1990; Poole, 2017) on how one's own knowledge interacts and contributes to their own and their family members' funds of knowledge. These accrued funds of knowledge are picked up through experiences interacting with technology. To develop effective privacy skills, children need experience going online *and* support from parents and others to understand how to avoid risky situations or cope when they occur (Wisniewski et al., 2015). Our typology reveals how different sources of information and experiences inform people's privacy practices in a way that the concept of privacy literacy does not. By working with low-income families and considering how they collectively develop privacy skills and knowledge, we address some of Hagendorff's (2018) concerns with the concept of privacy literacy and offer privacy funds of knowledge as a complementary framework.

Prior literature has identified underserved families as having the most to gain from leveraging funds of knowledge, given their limited physical access to technology and inadequate access to digital literacy instruction (Davis & Fullerton, 2016; Subramaniam, Scaff, Kawas, Hoffman, & Davis, 2018). Our findings regarding some of the less-protective privacy practices families described imply that they may not have accumulated sufficient funds of knowledge to develop safe privacy practices. We believe they will need to tap all sources of funds of knowledge to fill this void. Identifying people who bridge these funds of knowledge is also crucial. While Moll and Greenberg (1990) identified teachers and family members as bridges to bring funds of knowledge to the classroom, more research should explore who can be an ideal bridge to connect the multiple privacy funds of knowledge we have identified in this research. Our participants referred to librarians, technology teachers, and media teachers (school librarians) as sources of funds of knowledge for privacy, and each offers unique strengths for facilitating learning and knowledge development.

Developing Privacy Resources for Families

The broader goal of this research is to create resources to help families enhance their privacy practices. Prior work has found that few people attend privacy or digital literacy classes offered at public libraries (Vitak et al., 2018a), and that low socio-economic populations face unique challenges in managing privacy and developing effective privacy practices (Vitak, Liao, Subramaniam, & Kumar, 2018b). Our typology of privacy funds of knowledge can inform the development of privacy resources to help such families address these challenges. Our findings suggest a need to:

- Work closely with school systems and public libraries—which we identify as "community" funds of knowledge—to brainstorm ways to leverage technology lessons in schools and after-school library programs to help children enhance their privacy practices.
- Explore the potential of technology teachers, public librarians, and/or school librarians to serve as bridges that help generate privacy funds of knowledge in families. This could manifest as training on funds of knowledge and how they can be tapped to improve privacy practices.
- Develop strategic partnerships with local community experts in technology, banks, and libraries to co-develop and co-facilitate privacy learning. Community partners—especially those who are familiar with the challenges local families face—will be able to build trust quicker than outside entities. Likewise, having multiple community groups involved in this process will encourage wider awareness and participation.
- Co-create privacy resources using participatory design methods (Muller, 2009) with families and other sources of privacy funds of knowledge, including family friends,

extended family members, teachers, and librarians. Through participatory design, those who will use the resources will help design them, which allows the materials to better meet community needs.

LIMITATIONS

Since we did not design this study to explicitly identify privacy funds of knowledge, participants may have drawn on more sources than those they mentioned during the interview. Nevertheless, our data paints a rich picture of the variety of funds of knowledge that did emerge through our conversations with them. In addition, we specifically chose not to collect demographic information from participants to avoid asking invasive questions that may have prevented us from building rapport. Instead, we relied instead on the library branches' demographics as a proxy for socio-economic status and on the library staff to recruit families who fits the project's research goals. Finally, the interviews relied on self-reported data about participants' attitudes, opinions, and behaviors. We recognize that some participants may have been reluctant to share their experiences. We also recognize that family dynamics may have affected interviews. For example, children may have been less willing to discuss certain aspects of their technology use with a parent present; likewise, a parent might have been unwilling to talk about sensitive matters in front of their children.

CONCLUSION

This study extends the concept of funds of knowledge to privacy and explores how it can be used to enhance families' privacy practices. Researchers are investigating how children and families navigate and manage privacy and what challenges they face (Kumar et al., 2017); however, research on how and from where they develop privacy knowledge is still lacking. This study fills that void by illuminating the privacy funds of knowledge that inform families' privacy practices. Our findings can shape the pedagogical strategies used to help families better protect their privacy online and illustrate the positive roles that trusted community members can play in helping families do so. Future research is needed to design and develop these strategies in partnership with these community members.

ACKNOWLEDGMENTS

This research is funded by an IMLS National Leadership Grant, LG-81-16-0154-16. We thank the Maryland State Library Agency, as well as the coordinators at each library branch and at the Latino nonprofit for their assistance in recruiting participants and facilitating on-site interviews.

REFERENCES

Agosto, D. E., & Abbas, J. (2016). Simple Tips for Helping Students Become Safer, Smarter Social Media Users. *Knowledge Quest*, *44*(4), 42–47.

Barton, A. C., & Tan, E. (2009). Funds of knowledge and discourses and hybrid space. *Journal of Research in Science Teaching*, *46*(1), 50–73. https://doi.org/10.1002/tea.20269

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, *56*, 147–154. https://doi.org/10.1016/j.chb.2015.11.022

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online Privacy Concerns and Privacy Management: A Meta-Analytical Review: Privacy Concerns Meta-Analysis. *Journal of Communication*, *67*(1), 26–53. https://doi.org/10.1111/jcom.12276

Chen, Y., Carger, C. L., & Smith, T. J. (2017). Mobile-Assisted Narrative Writing Practice for Young English Language Learners from a Funds of Knowledge Approach. *Language Learning & Technology*, *21*(1), 28–41.

Davis, K., & Fullerton, S. (2016). Connected learning in and after school: Exploring technology's role in the learning experiences of diverse high school students. *The Information Society*, *32*(2), 98–116. https://doi.org/10.1080/01972243.2016.1130498

Givens, C. L. (2015). *Information privacy fundamentals for librarians and information professionals*. Lanham, Maryland: Rowman & Littlefield.

Hagendorff, T. (2018). Privacy Literacy and Its Problems. *Journal of Information Ethics*, *27*(2), 127–145.

Kajamaa, A., Kumpulainen, K., & Rajala, A. (2018). A digital learning environment mediating students' funds of knowledge and knowledge creation. *Studia paedagogica*, (4), [49]-66. https://doi.org/10.5817/SP2018-4-3

Kumar, P. C., Chetty, M., Clegg, T. L., & Vitak, J. (2019). Privacy and Security Considerations For Digital Technology Use in Elementary Schools. *Proceedings of the 37th Annual ACM Conference on Human Factors in Computing Systems*. Presented at the CHI, New York. https://doi.org/10.1145/3290605.3300537

Kumar, P., Naik, S. M., Devkar, U. R., Chetty, M., Clegg, T. L., & Vitak, J. (2017). "No Telling Passcodes Out Because They're Private": Understanding Children's Mental Models of Privacy and Security Online. *Proceedings of the ACM on Human-Computer Interaction*, *1*(CSCW), 1–21. https://doi.org/10.1145/3134699

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic Inquiry* (1st edition). Beverly Hills, Calif: SAGE Publications.

Livingstone, S., Haddon, L., & Görzig, A. (Eds.). (2012). *Children, risk and safety on the internet: research and policy challenges in comparative perspective*. Bristol, UK: Policy Press.

Mills, K. (2019). *Illuminating Children's Scientific Funds of Knowledge Through Social Media Sharing* (Doctoral Dissertation). University of Maryland, College Park, MD.

Moje, E. B., Ciechanowski, K. M., Kramer, K., Ellis, L., Carrillo, R., & Collazo, T. (2004). Working Toward Third Space in Content Area Literacy: An Examination of Everyday Funds of Knowledge and Discourse. *Reading Research Quarterly*, *39*(1), 38–70.

(International Reading Association, Order Department, P.O. Box 6021, Newark, DE 19714-6021. Tel: 800-336-7323 (Toll Free); Tel: 302-731-1600; Fax: 302-737-0878; e-mail: customerservice@reading.org.).

Moll, L. C., Amanti, C., Neff, D., & Gonzalez, N. (1992). Funds of Knowledge for Teaching: Using a Qualitative Approach to Connect Homes and Classrooms. *Theory Into Practice*, *31*(2), 132. https://doi.org/10.1080/00405849209543534

Moll, L. C., & Greenberg, J. B. (1990). Creating Zones of Possibilities: Combining social contexts for instruction. In *Vygotsky and Education: Instructional Implications and Applications of Sociohistorical Psychology*. Cambridge University Press.

Muller, M. (2009). Participatory design: The third space in HCI. In A. Sears & J. A. Jacko (Eds.), *Human-Computer Interaction: Development Process* (pp. 166–185). Boca Raton, FL: CRC Press.

Park, Y. J. (2013). Digital Literacy and Privacy Behavior Online. *Communication Research*, *40*(2), 215–236. https://doi.org/10.1177/0093650211418338

Petronio, S. (2002). *Boundaries of Privacy: Dialetics of Disclosure*. Albany: State University of New York Press.

Poole, A. (2017). Funds of Knowledge 2.0: Towards digital Funds of Identity. *Learning, Culture and Social Interaction*, *13*, 50–59. https://doi.org/10.1016/j.lcsi.2017.02.002

Rader, E., & Wash, R. (2015). Identifying patterns in informal sources of security information. *Journal of Cybersecurity*, tyv008. https://doi.org/10.1093/cybsec/tyv008

Redmiles, E. M., Kross, S., & Mazurek, M. L. (2017). Where is the Digital Divide?: A Survey of Security, Privacy, and Socioeconomics. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17*, 931–936. https://doi.org/10.1145/3025453.3025673

Smith, A. (2017). *What Americans Knows About Cybersecurity*. Retrieved from Pew Research Center website: http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/

Subramaniam, M., Scaff, L., Kawas, S., Hoffman, K. M., & Davis, K. (2018). Using Technology to Support Equity and Inclusion in Youth Library Programming: Current Practices and Future Opportunities. *The Library Quarterly*, *88*(4), 315–331. https://doi.org/10.1086/699267

Thompson, K. M., Jaeger, P. T., Taylor, N. G., Subramaniam, M. M., & Bertot, J. C. (2014). *Digital literacy and digital inclusion: information policy and the public library*. Lanham: Rowman & Littlefield.

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reforming European Data Protection Law* (pp. 333–365). https://doi.org/10.1007/978-94-017-9385-8

Turow, J., Bleakley, A., Bracken, J., Carpini, M. X. D., Draper, N., Feldman, L., … Nir, L. (2014). *Americans, Marketers, and the Internet: 1999-2012*. Retrieved from Annenberg School for Communication website: https://papers.ssrn.com/abstract=2423753

Turow, J., Hennessey, M., & Draper, N. (2015). *The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers And Opening Them Up to Exploitation* (pp. 1–24). Retrieved from Annenberg School for Communication website: https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf

Vélez-Ibáñez, C. G., & Greenberg, J. B. (1992). Formation and Transformation of Funds of Knowledge Among U.S.-Mexican Households. *Anthropology & Education Quarterly*, *23*(4), 313–335. https://doi.org/10.1525/aeq.1992.23.4.05x1582v

Vitak, J., Liao, Y., Kumar, P., & Subramaniam, M. (2018a). Librarians as Information Intermediaries: Navigating Tensions Between Being Helpful and Being Liable. In G. Chowdhury, J. McLeod, V. Gillet, & P. Willett (Eds.), *Transforming Digital Worlds* (pp. 693–702). Cham: Springer International Publishing.

Vitak, J., Liao, Y., Subramaniam, M., & Kumar, P. (2018b). 'I Knew It Was Too Good to Be True": The Challenges Economically Disadvantaged Internet Users Face in Assessing Trustworthiness, Avoiding Scams, and Developing Self-Efficacy Online. *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW), 1–25. https://doi.org/10.1145/3274445

Vygotskiĭ, L. S. (1978). *Mind in society: the development of higher psychological processes* (M. Cole, V. John-Steiner, S. Scribner, & E. Souberman, Eds.). Cambridge: Harvard University Press.

Wash, R., & Rader, E. (2011). Influencing mental models of security: a research agenda. *Proceedings of the 2011 Workshop on New Security Paradigms Workshop - NSPW '11*, 57. https://doi.org/10.1145/2073276.2073283

Wisniewski, P., Jia, H., Xu, H., Rosson, M. B., & Carroll, J. M. (2015). "Preventative" vs. "Reactive": How Parental Mediation Influences Teens' Social Media Privacy Behaviors. *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, 302–316. https://doi.org/10.1145/2675133.2675293

Wissinger, C. L. (2017). Privacy Literacy: From Theory to Practice. *Communications in Information Literacy*, *11*(2), 378–389.