“I Knew It Was Too Good To Be True”: The Challenges Economically Disadvantaged Users Face in Assessing Trustworthiness, Avoiding Scams, and Developing Self-Efficacy Online

JESSICA VITAK, University of Maryland, College of Information Studies[1]
YUTING LIAO, University of Maryland, College of Information Studies
MEGA SUBRAMANIAM, University of Maryland, College of Information Studies
PRIYA KUMAR , University of Maryland, College of Information Studies

In the U.S., consumers increasingly turn to the internet and mobile apps to complete essential personal transactions, ranging from financial payments to job applications. This shift to digital transactions can create challenges for those without reliable home internet connections or with limited digital literacy by requiring them to submit sensitive information on public computers or on unfamiliar websites. Using interviews with 52 families from high-poverty communities in the mid-Atlantic region of the U.S., we explore the compounding privacy and security challenges that economically disadvantaged individuals face when navigating online services. We describe the real, perceived, and unknown risks they face as they navigate online transactions with limited technical skills, as well as the strategies and heuristics they employ to minimize these risks. The findings highlight a complex relationship between participants’ negative experiences and their general mistrust of sharing data through online channels. We also describe a range of strategies participants use to try and protect their personal information. Based on these findings, we offer design recommendations to inform the creation of educational resources that we will develop in the next phase of this project.

CCS Concepts: • **Security and privacy** → **Human and societal aspects of security and privacy** → Social aspects of security and privacy

KEYWORDS

Privacy; security; low socioeconomic status; digital literacy; digital divide; marginalized populations; scams

ACM Reference format:

Jessica Vitak, Yuting Liao, Mega Subramaniam and Priya Kumar. 2018. “I Knew It Was Too Good To Be True”: The Challenges Economically Disadvantaged Users Face in Assessing Trustworthiness, Avoiding Scams, and Developing Self-Efficacy Online. In *Proceedings of the ACM on Human-Computer Interaction,* Vol. 2, CSCW, Article 176 (November 2018). ACM, New York, NY. 25 pages. https://doi.org/10.1145/3274445

1 INTRODUCTION

In the U.S. and around the world, people rely on mobile and Internet-connected devices to accomplish everyday tasks that include banking, shopping, submitting job applications, and getting breaking news updates. Driven by the popularity of social media, a significant proportion of research

This.is work is supported by the IMLS, under grant LG-81-16-0154-16.

[1] Corresponding author’s address: J. Vitak, Room 2117G Hornbake Building, South Wing, 4130 Campus Drive, College Park, MD, USA, 20742.

DOI: https://doi.org/10.1145/3274445

examining these technologies' impacts in the last decade has focused on their *social* uses—including how they reconnect old friends, enable new connections and romantic relationships, and ease the loneliness and isolation that is common among older adults. In more recent years, however, internet-related threats increasingly challenge individuals' digital privacy and security. For example, from 2012 to 2016, the U.S.-based Internet Crime Complaint Center (IC3) received more than 1.4 million complaints—many involving compromises of personally identifiable information (PII) through personal data breaches, phishing, identity theft, credit card fraud, or online harassment—for a total reported loss of US$4.63 billion [23].

Despite these risks, people with reliable home internet access and adequate skills to navigate online systems widely welcome the internet as a tool to complete various tasks. But for those with limited digital skills and/or no internet connection at home—or those with limited data plans or mobile-only connections through their phone providers—completing these tasks may become *riskier* as services move online. Having to use public computers or navigate complicated and confusing online programs may lead some people with low digital literacy to give up, submit incorrect information, submit sensitive information to the wrong company or person, or leave their personal information vulnerable to theft.

Recent discussions about the digital divide suggest that simply focusing on *physical access* to computers and the internet is insufficient; instead, we must consider the *quality* of that access [25] and focus on narrowing that gap. More than any other factor, one's socioeconomic status (SES) predicts home internet access, with the economically disadvantaged often having to turn to public libraries or other local organizations to submit job applications, apply for Medicaid and related federal services, and pay their bills. While skills likely range significantly within this population, research highlights that technology- and internet-related skills are lower among those with less income and education compared to the general population [13], [61], [63]. For the economically disadvantaged, lower levels of access to technology and lower levels of proficiency with technology could make it difficult to easily and accurately complete online tasks. They may experience increased privacy and security risks due to the nature of the devices they use (e.g., public computers) and their lower levels of knowledge about how to protect their data.

In this paper, we evaluate the challenges faced by economically disadvantaged internet users—an important but largely ignored population in empirical research—who increasingly need to complete financial, health, and other tasks through online systems. Two research questions guide our analysis:

RQ1: What challenges and/or barriers do economically disadvantaged Internet users experience when trying to complete tasks that require submitting personal information through online and mobile channels?

RQ2: What strategies and heuristics do economically disadvantaged Internet users employ to respond to online risks to the security of their personal information?

By exploring the challenges and strategies that low-SES internet users themselves identify, we can begin to understand how their privacy and security conceptualizations and values may differ from other populations and to identify where gaps between knowledge and practice can lead to increased risk. In this study, we focus on privacy issues related to individuals' PII and their knowledge (or lack thereof) of how to keep their PII safe and secure. We focus only on the attitudes, beliefs, and experiences that our participants volunteered about themselves—and their family members'—and their technology use. We use the terms "low-SES" and "economically disadvantaged" interchangeably to refer to the subset of the U.S. population that is living near or below the poverty line as designated by the federal government.[2]

This paper provides two main contributions to the CSCW community. First, we extend prior work on how individuals conceptualize online risks and their response to those risks when sharing information online [e.g., [70], [71] to a largely unstudied population. With one notable exception [37], researchers have largely left the study of how economically disadvantaged families respond to digital privacy and security challenges to the "future work" sections of their papers. Second, we take a sociotechnical approach to evaluating our data and propose clear recommendations for designing resources specifically for this population—which we will begin to do using participatory design methodologies in the next phase of this project. This approach will allow for more context-dependent and thoughtful solutions that are driven by the audiences for these tools, rather than through a more top-down approach that focuses on "average" users of a technology.

In the following sections, we provide an overview of research on the digital privacy and security risks that low-SES families face when using online tools and issues around trust in these communities. We then share results from interviews with 52 families from low-SES neighborhoods in Maryland, focusing on the challenges they identify facing when trying to successfully and safely using the internet, as well as the strategies they have developed to minimize risk. We evaluate these findings in light of prior work with populations that do not face the same types of challenges, and we offer recommendations for designing resources to help this population develop their digital literacy skills and well as their knowledge of online privacy and security.

2 RELATED WORK

Before discussing related research, we first define the main concepts of interest. We follow Park's [42] definition of digital literacy as "individual knowledge regarding computer-related functions" (p. 216). In operationalizing this concept, Hargittai [17] further distinguishes between one's perceived degree of knowledge—or self-efficacy—and their digital literacy, which can be measured through assessment of one's computer and Web-use skills. Digital literacy is intrinsically related to the digital divide; in fact, Hargittai [15] describes a "second-level digital divide" that refers not to technology access, but to one's degree of skill in using a given technology. Even when access is nearly universal, the skills divide between those with high digital literacy and those with low digital literacy negatively affects a range of social and economic outcomes.

2.1 The Impact of the Digital Divide on Online Risks and Self-Efficacy

The overall percentage of Americans who report having their PII compromised has steadily increased. The Data & Society Research Institute reported that in 2015, 27 percent of internet users said they had important data stolen [37]. Yet the risks and costs of being victimized by online threats are not borne equally. For instance, internet users in the lowest income bracket (i.e., households earning less than US$20,000 per year) are more than twice as likely as those earning US$100,000 or more per year to report suffering a financial loss due to an online scam or fraud [37]. In addition, Hispanics and those living in the lowest-income households are more likely to report encountering persistent and unwanted contact online. This includes contact from scammers or others trying to take advantage of people based on their immigration status, financial condition, or lack of technical or language proficiency. Low-SES internet users are more likely to say they have had an email or social

[2] In 2017, the Federal Poverty Income Level for a family of four was US$28,920; however, the amount of income needed to survive varies based on the region of the U.S. as well as other factors.

media account compromised and are more likely to report having their reputation damaged by online activity [45]. They are also more likely to express heightened concerns about their digital privacy and security [38].

While previous research has confirmed the existence of a digital divide—the gap between lower- and higher-SES populations in access to digital technology, as well as the gap in skills and knowledge about how to use such technologies [18], [48], [55], [59], [63]—very few studies have directly linked the phenomenon to security and privacy challenges. In one notable exception, Redmiles and colleagues [46] identified the first evidence of a "digital divide" in security, finding that users with higher skill levels and SES were significantly more likely to get digital privacy and security advice from coworkers and to say they learned from negative experiences online. The authors further suggested that this divide may increase the vulnerability of already disadvantaged users. Likewise, a recent Pew Research Center survey highlights a knowledge gap on issues around privacy and security; on a 13-item quiz, respondents with a high school education or less averaged only four correct responses, compared to seven correct answers for college graduates [41].

An important concept related to digital skills is self-efficacy, which speaks to individuals' belief in their ability to complete a task. Researchers have long considered the role that self-efficacy plays in narrowing or closing the digital divide skills gap [9]. Numerous efforts have sought to provide training and other resources to digital "novices" during the last 20 years, but recent research has found that attitudes reflecting low self-efficacy still pervade. For example, Madden [37] found that low-income social media users are less likely to feel they "know enough" about managing their privacy settings and are less likely to feel they have a good understanding of the privacy policies for the sites they use.

Beyond individuals' beliefs about their digital skills, researchers have also identified income-related differences in privacy-related behaviors. For instance, low-SES social media users are significantly less likely than higher-earning groups to have used more restrictive privacy settings when sharing content online [38]. They are also less likely to engage in privacy-protective strategies that may affect how they are tracked online, including turning off cookies [38]. Finally, low-SES internet users may not be in a position to pay a monetary fee to opt out of the collection of their phone or internet data [26]. Indeed, many have argued that privacy in the digital age is becoming a luxury good [19].

Looking beyond the U.S. context, scholars in the areas of information communication technology for development (ICT4D) and human-computer interaction for development (HCI4D) have examined challenges encountered by marginalized people in resource-constrained settings within the Global South. Vashishta et al.'s [67] research suggests that sociocultural values, lack of knowledge and awareness, use of technology in ways unintended by the technology designers, contexts in which a technology is used, and usability and cost considerations shape perceptions surrounding security, privacy, and confidentiality in developing regions. Among these factors, knowledge gaps—a form of the digital divide—is most relevant to current research. Likewise, in a study exploring internet security perceptions in urban and peri-urban Ghana, Chen et al. [5] found that people with lower computer skills were less likely to be able to perform security and privacy measures such as deleting text messages, cookies, browsing history, and emails. Additionally, most online systems and services often present information about their security and privacy practices (e.g., terms and conditions, privacy policy) in English and at a grade level that users with lower literacy levels cannot easily understand [4].

To summarize, differential access to digital privacy and security-related knowledge and uneven skill levels, coupled with a divergence in privacy-protective behaviors, likely renders low-income populations more vulnerable to online security risks. This population's lower levels of technical knowledge and skills may make it even more challenging for them to know when their behaviors endanger their PII.

2.2 Low-SES Communities and Trust

Trust is a central component of human interaction [1]; it functions to reduce the complexity people face [53]. Social trust is a belief in the honesty, integrity, and reliability of others—a "faith in people" [58]. In the absence of sufficient knowledge, people use social trust to guide their decisions and judgments [34], [35], [52]. Myriad studies have examined the role of trust in various contexts, including e-commerce activities [20], [27], [34], [47]], online interpersonal interactions [6], [8], [52], and evaluation of the credibility and quality of information searched online [11], [49], [53], [61]. Researchers have found that instead of making rational judgments based on knowledge, people use social trust to select experts who are trustworthy and whose opinions they consider accurate. For instance, people trust experts who share the values they believe are important for a given situation [2], [57], or trust a web source because of tabulated credibility (i.e., based on aggregated ratings provided by multiple users of a web service) or emergent credibility (based on pooled resources such as Wikipedia) [10].

However, low-SES communities remain understudied within this literature. In one exception, Mackert and colleagues [36] conducted focus groups with culturally diverse groups of parents who had low literacy levels. They found that some avoided websites with the suffix .edu or .gov because they viewed the sites as "too complex" or because they felt distrust toward government websites. In another, Subramaniam et al. [57] worked with tweens from economically disadvantaged backgrounds to understand how they assessed the credibility of information online. They found that factors such as limited English-language proficiency, a lack of familiarity with well-known sources, and preference of multimedia (over text) sources limited their ability to assess websites' credibility and trustworthiness.

Specifically looking at individuals' trust in institutions that regularly handle personal data, Madden [38] found that low-SES individuals were less likely than higher-SES groups to say they trust their internet service providers (ISP), cell phone providers, and law enforcement agencies to protect their personal information. Those with lower levels of education were considerably more likely to doubt their ISP's ability to protect their personal information—48% of online adults with less than a high school degree said they trust their ISP "only a little" or "not at all," compared with 33 percent of online adults who are college graduates. Additionally, foreign-born Hispanics expressed the lowest levels of trust in cell phone providers [38]. While this work did not evaluate why these differences in trust emerged, we find this to be an especially telling data point given how much data ISPs collect, how reliant low-SES populations are on their mobile device—as it may be their primary or sole way to connect to the internet and complete essential online transactions—and how recent legislative changes have given ISPs more freedom to commercialize user data [28].

Another important topic related to this population is the role of librarians. As information intermediaries, librarians help patrons exchange and disseminate PII, translate technical information, and make information easier to use [59]. Vitak et al. [68] found that patrons seem to inherently trust librarians when it comes to handling PII. For marginalized groups, including immigrants and low-

SES individuals, libraries may be one of the only trusted resources in their local community [65], [66].

2.3 Developing Models and Heuristics of Privacy and Security

To ensure people use the internet in a way that protects their privacy and security, those who design technologies need to give users sufficient options to achieve privacy. Conversely, those who use the technologies need to be able recognize—and address—potential security threats relatively easily. Entire conferences focus on the development of privacy-enhancing technologies (e.g., PETS) and usable privacy and security solutions (e.g., SOUPS). But aligning the two can be difficult. For example, computer security professionals advise that internet users take the following steps to protect themselves online: keep their device's operating system and applications up-to-date, use a password manager that contains strong and unique passwords, and turn on two-factor authentication [24]. On the other hand, everyday internet users believe the best strategies to protect themselves online are to use antivirus software, create strong passwords but change them frequently, and only visit trusted websites [24].

Promoting privacy- and security-protective decision-making involves more than simply giving people information about threats and telling them what to do [26]. It requires understanding what mental models shape people's perceptions of what online threats exist, what actions would protect them from such threats, how vulnerable they feel they are to such threats, and whether they feel the threats are worth addressing [70]. Furthermore, people's models likely differ based on demographic factors such as age or education level. For example, internet users with less education are more likely to believe that there is nothing they can do to protect themselves from viruses or hackers and less likely to take protective actions, while those who are older or have higher education levels report taking more protective actions but also do not consider themselves to be vulnerable to online threats [72]. In addition, people may absorb different lessons about online security depending on the source of information. Personal anecdotes can be powerful tools to make security lessons resonate [71], but expert advice websites may be a better source for information on how online attacks happen and how people can protect themselves [72]. In addition, people may misunderstand how privacy and security concerns differ or remain the same between laptop and mobile device use [7], and they may feel more comfortable with data collection when they understand its purpose [32].

The research in this space emphasizes that interventions to promote privacy- and security-protective decision-making must consider more than a person's knowledge. The goal is not to evaluate whether people's mental models are correct, since incorrect models can still lead to desirable outcomes, but rather to understand how people's models contribute to certain behaviors [71]. For example, if a person's mental model says computer security tools are useful, then the challenge is to make them usable; however, if their mental model says computer security tools are unnecessary, making them usable will not encourage adoption [71]. Demographic factors, perceptions about vulnerability, motivations for internet use, the type of device people use or online activity in which they engage, and their awareness of the purpose of data collection all influence how someone behaves online. In their meta-review of end-user computer security research, Howe et al. [22] call on more studies to consider the role of socioeconomic status on decision making related to online security. We offer this study as a step in that direction.

3 STUDY CONTEXT

This paper is part of a larger project funded by the Institute of Museum and Library Services (IMLS) and conducted in partnership with Maryland's Division of Library Development and Services (DLDS). The first goal of the project is to evaluate the challenges that low-SES families face as they navigate online transactions that involve PII, and the challenges that information intermediaries (such as librarians) face as they assist with such transactions. The second goal of the project is to develop educational resources for low SES-families to reduce risky behaviors and enhance overall privacy-related digital skills, and to help librarians and other information intermediaries better support low-SES families.

We are embarking on the second year of this project, which entails analyzing data collected in the project's first year. We recently reported findings from focus groups with 36 librarians to determine the challenges librarians face serving as information intermediaries to low-SES families [68]. Here we present data from interviews with 52 families to determine privacy and security challenges they face when using the internet to transmit sensitive personal information. Specifically, we discuss challenges associated with trustworthiness, scams, and self-efficacy from a subset of the family interview data (see Method section for more details).

The second and third years of this project are dedicated to developing the resources mentioned above. We will conduct a series of participatory design activities that include ideating, designing, and prototyping these resources with low-SES families and librarians, pilot testing these resources, and disseminating them broadly in the U.S. The project is expected to provide tools that can librarians can used to inform their practices in helping families complete sensitive online transactions and to facilitate digital privacy and security skills education for these families.

4 METHOD

To recruit participants, we first identified four library branches in Maryland in high poverty communities. Table 1 includes details on the branches, their general location, and common socio-economic markers associated with poverty. Note that we tried to span both more rural and urban locations, with one branch located in a large city, one located directly outside a large city, and two located in very rural parts of the state.

Table 1. Descriptive Details for the Four Partner Library Branches[1]

Branch[2]	Location	Approximate Pop. (3-mile radius)	% of Pop. That Completed College	% of Pop. That Is Unemployed	% of Pop. Below Poverty Line
A	Rural	3,000	16%	14%	28%
B	Urban	112,000	33%	12%	24%
C	Urban	97,000	20%	17%	20%
D	Rural	2,000	15%	11%	20%

[1] Data based on the 2014 Digital Inclusion Survey. See https://digitalinclusion.umd.edu/content/2014-survey-results-and-reports

[2] Branch names have been anonymized and data have been rounded to avoid identification.

After identifying our research sites, we worked with library branch managers and librarians to identify participants. The research team created fliers and shared details of the study with library staff, and they recruited patrons who fit our study goals. We conducted interviews with 46 families on site at the four libraries between March and May 2017. Interviews ranged from 25 to 75 minutes. We also partnered with a local, non-profit Latino and immigration advocacy organization to recruit participants who offered perspectives from immigrant populations and those who speak English as a second language. During June 2017, we interviewed six additional families at a public center run by this organization in a suburban region of the state. All interviews included at least one adult; however, we encouraged multiple family members to attend interviews to obtain a variety of perspectives from each family unit. In total, we spoke with 54 adults and 23 children from 52 families (13 identifying as Latino) over three months. When children were present, we asked additional questions about their technology use at home and school and whether they had learned about online safety or security in school settings.

English-language audio files (n=37) were transcribed using the online service Rev.com, while Spanish-language audio files (n=7) were translated and transcribed using the company Verbal Ink and an independent contractor. We imported the transcriptions into the qualitative software analysis program Dedoose and used an iterative process to develop and refine the codebook. First, we created an initial codebook based on the interview protocol and research goals. Each author separately coded one interviews using the initial codebook. We discussed the coding process and refined the codebook, adding, deleting and merging codes. We repeated this process with a second interview, finalizing the codebook in a follow-up meeting [33].

The final codebook contained 24 codes, including codes for adults' or children's attitudes (e.g., adult privacy concerns, child privacy concerns) and behaviors (e.g., adult privacy/security behaviors, child privacy/security behavior). The codebook also included codes for technology literacy, trust in online sources, and definitions of sensitive information, among others. The Appendix presents an abbreviated version of the codebook. Each transcript then went through two rounds of coding: a primary round in which an author applied the codes and a secondary round where another author confirmed the coding decisions made during the first round.

To address this study's research questions, we focus on excerpts from three codes: (1) security threats/scams, which captured participants descriptions of experiences that they or people they knew had with online scams or threats to personal information—as well as experiences that could have been scams but weren't framed as such; (2) trust/lack of trust in online sources, which captured comments describing how much a participant trusted or did not trust technology generally, as well as references to specific companies or sites (e.g., Google) and why they felt this way; and (3) trust in librarians, which captured comments related to participants' feelings about sharing information with or asking help from a librarian when using library services. Participant quotes and comments presented in the findings section are identified by where the interview took place: at one of the four library branches (with a letter preface of A-D, based on the library branch data presented in Table 1), or with the preface "LN" to indicate interviews conducted at the Latino non-profit advocacy organization.

4.1 Considerations for Working with Low-SES populations

A major motivation for conducting this research project was our observation that there is a dearth of research looking at privacy and security challenges among—and solutions targeted toward—economically disadvantaged individuals and families. These groups face additional challenges beyond those often discussed for more "average" Americans due to their income, education, technology skills and access, immigration status, English language proficiency, and other factors.

This population is also especially vulnerable to being targeted by scammers and others looking to take advantage of people that lack the knowledge or resources to address potential threats. When designing our study, we took care that our research respected the population and did not impose additional burdens on them.

We partnered with Maryland's state library agency and, by extension, the four library branches, as well as with the non-profit Latino advocacy organization, in large part because of their familiarity with low-SES communities in the state. We relied heavily on their knowledge of the local community and library patrons to help us identify likely participants. Going through the organizations to recruit participants, rather than trying to recruit directly, helped us establish trust and rapport with community members and assuaged potential concerns about the research. Conducting the research in these public spaces also likely eased concerns.

When conducting the interviews, we specifically did not collect identifying information from participants beyond that required for the consent forms. In many cases, participants volunteered information about themselves and their backgrounds when responding to questions; however, due to the sensitive nature of the research and the population, we determined that directly asking them for demographic information might make participants uncomfortable and less willing to share their stories with us. Instead, we use demographic data for the communities around each library as a proxy for our participants' socio-economic status.[3] While this provides a less rigorous accounting of the specific background of each participant, we believe this choice yields a richer dataset. Furthermore, by using librarians as our primary participant recruiters, we could ensure that the majority of the participants were regular patrons who lived in the neighborhood and regularly used the library's services.

Finally, our funding agency, IMLS, prompted us to pay participating families a US$75 cash incentive. The rationale for this amount was that our participants are economically disadvantaged, and we should generously compensate them for providing us with important insights that would otherwise be difficult to obtain.

5 FINDINGS

5.1 RQ1: Assessing Technology Challenges and Barriers

As we talked with families about their use of technology and the challenges they faced in using technology safely and effectively, a number of themes emerged. Below, we discuss how threats crossed communication channels and how the boundaries between "offline" and "online" spaces frequently become blurry, especially with mobile devices. We also describe how many families found it difficult to determine whether a potential threat was real or imagined.

5.1.1 Multi-channel threats. Our participants described a range of scams they had encountered personally or heard about from others in their social circle. Examples of fraudulent behavior and security threats included phone scams, stolen credit card information, computer viruses, compromised email or social media accounts, online stalking, and false transactions.

One of the most frequent threats that arose were phone scams, where callers requested personal information or money. Several participants described receiving calls from people pretending to be technical support and offering to fix computer problems. Other phone scams involved luring victims

[3] Participants were asked if they were interested in being contacted about participating in future phases of the research project and, if so, entered a phone number and/or email address on their consent form.

with purported lottery winnings or other monetary rewards. Many participants who received these calls said they quickly realized the calls were “too good to be true" or had obvious red flags that signaled a potential scam; however, some described feeling uncertainty and confusion at the time.

For example, participant A3, who hailed from a more rural part of the state, said she received many calls from strangers who asked her questions; she attributed these calls to her frequent use of online job sites like Indeed and Monster. She described getting a call where she was told she’d receive a US$100 Wal-Mart gift card in exchange for a small credit card payment (US$1.95) and she agreed. However, she noticed multiple charges on her account for much more money over the following weeks. She said, “*My bank was like, ‘Well you need to be a little bit more careful.’ I was like, ‘I know but it just sounded so good.’*” Other participants talked about more general experiences of getting spam phone calls from strangers saying they owed them money. When asked how she thought these people got her cell number, participant A9 replied, “*I think that they still sell numbers. It’s illegal now, but I think they still do it.*”

The second category of threats that came up in our interviews involved participants’ internet use and viruses/hacking, including having email or social media accounts compromised, online stalking, and fraudulent online transactions. In the more extreme cases, these scams involved losing money. Participant A6 described a friend’s experience by saying, “*they were on [their laptop] researching something and then the whole computer went black and said, ‘If you pay us US$300, we will fix your laptop,’ or something crazy*.” Participant B7 said a family friend was attacked violently and robbed of US$4000 when he tried to sell a used car through Craigslist. Likewise, many of our participants described examples of having credit card information stolen or compromised and experiencing negative financial outcomes. As we discuss below when examining RQ2, the uncertainty around questions like this may lead people in this population to hesitate submitting PII—and especially financial information—through any online channels, including legitimate ones.

Third, we found examples of threats that highlighted how subsections of this population were even more vulnerable than others to be targeted by scams. These included older adults, people in debt, and immigrants. As noted in the Method section, we spoke to a number of immigrant families as part of our data collection, and for some, heightened concerns about speaking to law enforcement kept them from reporting scams or financial loss. For example, participant B9 from Mexico recounted how his parents received a fraudulent call from scammers pretending to be law enforcement: “*They [scammers] called [my parents] and told them they had me. And my mom called me and I said, ‘No, no one has me. Stay calm, everything’s fine.’ So that’s why it’s better not to post personal things on social media*.”

Likewise, participant A3 described how her friend, an older woman who had significant financial debt, was nearly scammed out of US$5000 by someone who pretended to be the debt owner: “*If there weren't anyone there, she would have [sent the money], would have given them all her information and everything. She thought that's something she owed. But see, she had dementia and she couldn't remember. So, they prey on weak people, like, a lot.*” In these cases, the combination of being poor and belonging to another vulnerable group made one a particularly tempting target for scammers.

5.1.2 Struggles to protect themselves from or respond to security threats. Analysis of the interviews revealed that many of our participants face challenges when determining how to protect themselves from online risks. Some also struggled to respond to threats such computer viruses and email account hacks. For instance, after participant C10’s email account was compromised and used to send out spam emails. When asked how she dealt with the situation, she replied: “*I think I just go through and*

I delete my junk mail very often... I guess that's all to do." She said she did not take any measures to update her account settings (e.g., changing her password). Similarly, several other participants described feeling helpless or unsure how to react after discovering their home computer had been infected with a virus or malware. For example, participant A2 described an experience she had, saying:

> "It was some type of weird Trojan, and it wouldn't let me do anything. I had to shut it down, and I was able to get back on it, and it showed back up even after I had the Norton virus thing on there. As far as technical stuff like that, I don't know anything, how to work it on the computer. I don't know how to fix it." (Participant A2)

Additionally, we found that participants sometimes engaged in behaviors that could make them more vulnerable to scams. For instance, participant A9 said she stopped using a traditional bank after she unknowingly deposited a fake check into her account, which triggered an investigation:

> "I didn't use any of the money or try to use any of the money. [The bank] just picked up on it, you know. In about a day or two, they called and was like 'Where'd you get this check from?' They asked me a whole bunch of questions. I'm like, I don't know too much about it. They told me, 'Your account's under investigation, blah blah blah.' So I said, you know what? I'm just not going to do that anymore. Yeah, so after they closed their investigation, I closed the account." (Participant A9)

Participant A9 decided to use the Green Dot prepaid card and mobile app for her banking needs. Green Dot cards can be used to "reload other prepaid cards, add money to a PayPal account without using a bank account, or make same-day payments to major companies" [40]:1]. Since the cards can only be purchased with cash, they enable people to spend money without revealing any personal or financial information. However, scammers also use these cards to defraud people; the New York City Police Department has alerted the public to watch out for such schemes [40]. When used legitimately, Green Dot cards actually offer more privacy than traditional banking and credit card companies. However, Green Dot lacks the security protections, such as fraud alerts, that are standard at institutional banks. Participant A9 closed her bank account out of frustration with the service, but it is unclear whether she considered the security implications of switching to Green Dot. This anecdote exemplifies why resources for helping people develop skills related to privacy- and security-related decision-making must be contextualized in people's everyday lives. After all, privacy and security are not one-size-fits-all concepts.

5.1.3 Resignation, fear, and perceived low self-efficacy. In addition to the negative experiences, financial loss, and emotional stress resulting from internet-related scams, we also observed a type of secondary victimization among some participants that led them to adopt negative attitudes toward technology. Some participants described various ways in which they directly or indirectly "rejected" technology because of concerns that someone could steal their information. Instead of submitting sensitive information online, some participants preferred to apply for government benefits by going to a local office, to submit job applications in person, to receive information in the "old paper format," or to process transactions in cash. For instance, participant B17 expressed how uncomfortable she felt about companies moving to online-only job applications:

> "Unfortunately, most [employers] today want you to apply online...I really don't have much of a choice... But you know what? Even with a paper application. Your information can still be stolen. It can be copied on a copy machine. But I try not to be that paranoid about it. I'm like, 'This is a risk you take. You need a job. You have to take the same risk as somebody who's going to get your information.' But I do have concerns, especially about online." (Participant B17)

For some participants, this concern was compounded by a fear of technology in general. Assuming that technology use always leads to bad outcomes may understandably make some people less willing to participate in online activities they perceive as risky, such as banking or applying for a job online. Some participants expressed frustration with the transition from paper to digital processes. Participant C6 stated:

> "I prefer the old paper format [for transactions] myself… [Because we're increasingly shifting services online], that might not be an option; I'm very, very scared. You have no choice. They give you no other option. No other option. You can't avoid it. But it is very scary because it will be antiquated, they probably won't accept money very shortly. Everything will have to be done on credit cards, which makes you vulnerable at everyone's disposal. Somebody could hit a button and destroy your entire life." (Participant C6)

For other participants, hesitation to use technology appeared to stem from a lack of self-confidence or knowledge of how to protect their information. Participant A5 described why she had not set up a PayPal account for online shopping, saying, "*I'd be afraid to do that. I'd be afraid I'd have something screwed up and they'd get my bank card number, and I'd have it all messed up.*" Perceived low self-efficacy related to protecting information privacy and security is especially problematic as processes such as applying for social services or jobs are shifting online. These comments highlight how resignation, fear, and perceived lack of self-efficacy related to protecting one's information online present barriers to technology use.

5.2 RQ2: Strategies and Heuristics Used to Minimize Risks Online

In evaluating our first research question, we found that participants experienced a range of security threats when using the internet and their mobile devices. Many described having limited technical knowledge and skills, while others avoided technology use as much as possible. These findings hint at some of the main strategies and heuristics our participants described using to navigate technology. Below, we describe the three main themes that address our second research question. We focus on participants' distrust in online sources, reliance on informational cues of trustworthiness, and whom they turn to when they need help.

5.2.1 Trust what you know—and don't trust anything else. In general, our participants' attitudes toward online risks fell into one of two camps. First, a large subset of participants said they distrust all online sources, often because they lack confidence in their ability to distinguish between threats and trustworthy sources. As we noted above, this distrust can be associated with rejection of technology, so many of these participants are more than willing to go out of their way to avoid online transactions. One mother, participant D3, described why she refuses to pay bills online:

> "I pay to do my banking in paper like in the mail. I just don't trust it. There's been too many hackings with government applications and then they hack into like credit card people or they accidentally send out their mailing list to like you and you get like a mailing list of like 10,000 people in your email. There's just too many mistakes being made. Not enough security where it needs to be. I don't care how good your password is. I just think there's probably spyware out there or people hacking into it. I just don't think it would be safe. Even then, they wouldn't get more than US$20 out of my account. It's not like I'm on a millionaire, but I just think that the possibility that it would be there for them to hack into at some point, some place and once it's in there, it's in there forever." (Participant D3)

Another mother (C12) we spoke to, who expressed extreme distrust of companies and people in general, described a commonly used reason to avoid these technologies. In describing her concerns about her personal information, she said, "*I don't feel secure at all. Whether somebody tells me, 'Oh, it's safe,' I don't trust that because anybody can hack into somebody's computer. Anybody can hack into anything. If they can do it to the government, they can do it to us.*" She then talked about how she avoided applying for jobs that required online applications and told her children not to share personal information when they played games online. She also refused to use social media, saying, "*No. I don't need Facebook. I mean if I'm going to see that person, I'll go see them. I don't need to go onto Facebook where everybody in the United States can see it.*"

This distrust of the internet was a common refrain from our participants. In another case, participant C6's teenage daughter said she wished there were more resources to help her tell "*the difference between a good website that you can trust and ones that you can't trust, because it's hard for me to tell the difference.*" Participant C6 then jumped in, saying you can't really trust any sites because a good hacker could "*doctor*" any site. In the end, she said, deciding whether to use an online service is a "*leap of faith*" and you have to rely on "*trial and error*" to determine whether a site is trustworthy or not.

Participants also used the heuristic of "trust what you know," when considering whether to share sensitive information online. When probed, they explained that this meant they were more likely to trust large companies such as Google, Wal-Mart, or Amazon, with whom they were familiar or had a history of transactions. Participants explained that these companies had a greater incentive to protect user data. Participant C4 described this when talking about why she should probably start backing up her phone: "*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.*" Others say they trust the "*big*" vendors but are more skeptical of new players, as Participant B3 noted when she said, "*I'm [comfortable using Amazon] because it's a trusted vendor. I mean, I trust that there are security measures... if I got an ad saying, I don't know whatever, some kind of percentage off, and I've not heard of the name, or it's very new or not new but it's a trend like Blue Apron, [I wouldn't].*"

Conversely, participants described numerous cases where they could sense when something was *"too good to be true*" and avoided a potential scam. This strategy reflects a heuristic of "trusting your gut." In one example, Participant A8 described finding a car online and wanting to buy it. She decided to do some research after the buyer wanted her to use eBay and said the car was in a warehouse somewhere. She said, "*Then I started typing some of the information [into Google], and everything popped up, scammer, scammer.*"

5.2.2 Look for informational cues of trustworthiness. We asked participants what—if anything—they did to reduce the chances of putting their personal information at increased risk when using the internet or their mobile devices. While some expressed little to no knowledge of how to do this, a number of our participants—and many of the children we talked to—described looking for various informational cues that suggested whether websites were trustworthy. These cues included HTTPS, the lock icon next to the URL, or the URL extension. For example, when asked how he knows how to trust a website when he visits it for the first time, participant C9's middle school-age son said:

> "I think the little green shield or something on the little website thing that says if it's secure or verified or something like that. Then there's ones with red and it's got a X through it or something, it's not secure, or something. I don't know. I know the green ones usually are secure." (Participant C9's son)

Others noted that a search engine would alert them if a website was untrustworthy. Participant LN2 said, "*My Google, it lets me know if it's a trusted website. If they have a certificate or something, they let me go to the website.*" On the other hand, participant LN3 described taking a class "*where they told us that for us to know whether a website is trustworthy, we have to look if it says '.org.' for an organization, and also for the government, it's '.gov.' They told us those are trustworthy sites.*"

Such informational cues may make it easier for a person to make privacy- and security-related decisions, but understanding what the cues mean still requires a certain level of digital literacy. For example, HTTPS can protect users from a man-in-the-middle attack, but it does not help detect a spear-phishing message. Thus, informational cues are most effective if people can connect them to a particular type of threat—something we did not observe our participants discussing.

5.2.3 Searching for answers outside one's network. Simply accessing a digital tool may not help a person who lacks the necessary skills to use it. This "second-level digital divide" [15] creates additional barriers to using digital technologies safely and successfully. Participants described experiences where they were confused or unsure how to solve a tech-related problem, ranging from setting up an online account to removing a virus from their home computer. Many participants described their friends and family as having similar technical skills as them, suggesting they may not be sources of help. Some participants said their older children were helpful with basic tech-related problems, like scanning documents or doing online searches, and several children mentioned they received at least some computer training at school.

Participants who could not rely on family or friends for help often turned to library resources or librarians. Due to the nature of this research project and the location of the majority of our data collection, this is unsurprising. However, public libraries are one of the most frequented locations for those without reliable access to computers and internet services because they typically offer access to free WiFi, low-cost printing services, and librarians who can assist them when they run into problems.

There is also evidence that the public has high levels of trust for both libraries (the institution) and librarians (the professionals) [14]. Our participants echoed this. They saw libraries as reliable sources of computers, internet access, and other resources (e.g., printers, scanners). Participants described using library computers for completing important tasks (e.g., submitting forms, paying bills), as well as an outlet for them and their children to relax. Using a library computer also reduced some concerns about security. Multiple participants said they trusted library computers more than personal computers because they knew library computers had up-to-date anti-virus software as well as tools that would delete files, log out accounts, and/or prevent other patrons from being able to access their personal information.[4] For example, participant C12, who expressed significant concerns about the safety and security of her information online, said she is much more comfortable submitting it at the library: “I won’t go nowhere else because I feel more safer now because the librarian lady told me it erases [my data from the computer].”

When considering interactions with librarians, participants’ comments reflected an implicit sense of trust. This echoed findings from our research with librarians in an earlier phase of this research project [68]. When asked why they trusted librarians with their personal information, most participants referenced librarians’ knowledge and personality. Regarding knowledge, many participants said they had turned to librarians for assistance using the library’s computers, as well as for help with specific websites or online tools. In other cases, participants said they had developed personal relationships with librarians over time and trusted them because they knew them well. Participants described librarians and their responses to technology help requests as *“helpful”* (B14), *“well-versed”* (B16), and *“patient and understanding”* (C5); participants appreciated when librarians didn’t make them feel “*dumb*” for not understanding basic computer terminology. Participant A14 summarized this by saying:

> “They usually have a mixture in age in staff, which helps out a lot. Even if someone may be new or just came on board or may not have experienced X, Y, Z issue, it's really not an issue because it’s never one particular person…. With all of their skills combined, it gets done. I never left the library where I was thinking, oh my god, I didn’t know how to do this and I came here for nothing.” (Participant A14)

A final theme that emerged from our dataset was specific to the subset of Latino participants who had limited English language skills. In these interviews, participants also expressed trust in librarians, but said their level of comfort in asking for help—especially regarding sensitive information—was lower when they had to interact in English than when they were able to speak with a librarian in their native language. For example, when asked if she trusted the librarians she interacted with, participant LN4 said:

> “Well yes, when it’s looking up something for my kids’ homework, yes, I trust them when I ask for help. But if it’s regarding some type of communication... for example, I had a problem once when I wanted to watch a video of my brother’s accident, so for things like that, I don’t trust asking for help as much because sometimes you feel bad. Like when it’s something more private…” (Participant LN4)

Importantly, when the interviewer asked if the participant would have felt more comfortable had the librarian spoken Spanish, she immediately said yes, saying that was because she would not be concerned about misunderstandings or miscommunication. Other participants viewed the language barrier as less of a problem, saying there was always or almost always a Spanish-speaking librarian working at their branch or because they had access to an information intermediary like a child who could help translate. That said, this case raises an important challenge for patrons who are English language learners using English-dominant websites, especially sites that require submitting sensitive information.

[4] It is important to note that, in some cases, this belief may have been misplaced, as individual library policies and practices regarding computer software vary widely and there is little to no standardization across branches or regions. This could be problematic if a patron visits more than one branch and each follows different computer data storage and deletion policies.

6 DISCUSSION

Technological innovation and the development of new tools and services have increased the ease and convenience with which people complete a range of tasks. Researchers in the CSCW community have been at the forefront of studying how sociotechnical systems emerge, are adopted, and succeed or fail within their userbases. Several scholars have also raised important questions about the privacy and security challenges these systems create, especially as they encourage people to share sensitive personal information directly or indirectly without a strong understanding of who will have access to that data, why they need access to that data, and how that data will be stored [32], [69]. The lack of transparency in how data flows from consumers to companies and/or the government is likely a major reason why studies show heightened distrust toward entities that collect, share, or otherwise use data from consumers and citizens [37], [45]. In addition, existing computer security resources focus largely on phishing and spam, data breaches, and viruses and malware, and devote the least attention to mobile privacy and security [43].

While privacy and security attract more attention in the post-Edward Snowden era, the focus of empirical research has not been equally distributed. Many studies that evaluate people's privacy concerns and security behaviors sample younger and more tech-savvy users, such as college students or Mechanical Turk workers. Even more general internet recruitment techniques bias samples toward those who have internet access and are likely to peruse the sites where advertisements are posted. What often happens—in research on this topic as well as many others—is that more marginalized subsets of the population (such as low-SES individuals) are left out of the data collection and analysis process, or they represent too small a proportion of the dataset to draw meaningful inferences. In looking at how individuals develop mental models around online information sharing, privacy concerns, and security behaviors, researchers have called for more research using diverse populations, especially those of low-socioeconomic status [22].

The primary goal of this study was to extend prior work examining the relationship between disclosing sensitive information through online systems and the concepts of trust, self-efficacy, privacy, and security to an understudied subset of the U.S. population—people who are economically disadvantaged. At a basic level, this classification speaks to annual income, but this status is typically correlated with a number of other factors that put this population at a disadvantage when it comes to technology access and skills. A 2016 Pew Internet report on the digital divide used survey data to create a typology of five categories of "digital readiness"; among those least prepared to adopt new digital technologies were women, those age 50 and older, those in lower income household or with lower education levels, and minorities [21]. People at the intersection of two or more of these identities are more likely to have negative experiences online (e.g., being targeted by scams) and to miss out on beneficial services like free online training programs.

The families we spoke to highlight the complex challenges these populations face in both accessing and successfully navigating technology to complete an increasing range of tasks through digital channels. Our participants faced threats from multiple channels (e.g., phone calls, mobile internet browsing, public computer use). Many detected when phone calls or online offers were "too good to be true" and responded accordingly. But they struggled to respond to threats directly tied to internet use, such as compromised email or social media accounts. For some, resignation, fear, or perceived low-self efficacy posed barriers to addressing privacy and security concerns. This echoes Wash and Rader's [72]:319] finding that American internet users with low levels of education were "least likely to believe it is possible [to] protect their computers from viruses and hackers" and "least likely to report taking any kind of protective actions related to viruses or hackers."

Tasks that more educated and affluent people may take for granted—like their child needing to do research on bird migration patterns for a homework assignment or searching for job openings using Indeed.com—require much more coordination when one lacks physical access and/or skills to accomplish those tasks on their own. Likewise, when faced with potential threats, such as a device becoming infected with a virus or a website appearing untrustworthy, our participants were less likely to have dedicated people or resources to whom they could turn for support and assistance. Perhaps because of this, we found that a number of our participants were hesitant to use technology or outright shunned it, preferring to use analog methods for submitting applications, forms, and payments whenever possible—even when that decision carried additional financial costs or took longer.

We want to ensure that people do not fear or distrust technology outright, but how do we best address the challenges raised by participants in this study? Wash and Rader [72]:319] conclude that "emphasizing vulnerability and using scare tactics is unlikely to help younger or less [educated] users, since they often don't believe there is anything they can do about [security threats.]" Many of our participants already expressed frustration, fear, or a perceived lack of self-efficacy related to technology. Solutions that belabor those points run the risk of alienating the very people they seek to help. Any successful solution will need to be nuanced and, as other researchers have noted, simply building technological tools, deploying them at public libraries, and hoping for the best will not work [26]. Part of developing successful solutions requires understanding how a population makes sense of technology [70]—in this case, what participants see as barriers or threats to using the internet, how serious they view privacy and security threats, and how much they would value taking steps to actively reduce those threats. In the following sections, we describe how we plan to work with this population over the next two years to jointly develop workable and implementable solutions.

6.1 Implications for the Design of Educational Resources for low-SES populations

As mentioned in the Context section, the research questions we explored in this paper are part of a multi-year project with the goal of developing educational resources to help low SES-families reduce risky behaviors and enhance overall privacy-related digital skills, and to aid librarians and other information intermediaries to better support the low-SES families in their communities. Based on our framing of digital literacy as individuals' understanding of how computers and the internet work [42]—as well as participants' comments describing themselves as having low levels of digital skills—our findings suggest that reduced digital literacy among economically disadvantaged Internet users may serve a as barrier to understanding the intricacies of privacy, practicing preemptive and reactive safe privacy behaviors, and trusting online websites and/or information intermediaries.

In terms of designing resources to help low-SES families to develop skills, enhance knowledge, and build self-efficacy, we believe that simply offering classes or training such as a session on "how to detect scams" or "how to detect fake websites," will not be sufficient to propel them toward behavioral change. Indeed, people may avoid following this type of advice, no matter how practical or actionable, because they don't think it will help them [70]. We do not want to prescribe specific guidelines; rather, we want to encourage these individuals to develop their own strategies and mental models of privacy and modify them as they develop their digital literacy skills. We came to this conclusion after librarians conveyed to us that low SES-families often prioritize immediate needs to complete online tasks rather than taking a long-term approach towards learning the skills needed to manage online risks and threats [68]. As mentioned above, it became evident that low-SES families often perceived librarians as neutral entities; hence, they trust—and may expect—librarians to complete tasks on their behalf that involve PII. While librarians have attempted to offer programs and sessions to teach patrons to assess threats and protect their PII, these sessions are often not well attended [68]. Therefore, we believe we will need to discern what type of resources and facilitation will be most useful for low SES individuals, and in what structure and format. These resources and facilitation techniques must also be something that librarians or other information intermediaries can potentially use as a teaching tool when a patron comes to them with a task or issue that involves PII. Such resources, with facilitation by librarians, will shift the perception of librarians as the trusted person who will complete tasks that involve PII on behalf of their patrons to the trusted person who guides the patrons on how to protect their PII.

Stories offer a promising vehicle for delivering privacy and security-related information [44][71]. Our participants frequently shared stories of privacy and security-related experiences that they had heard from others; some acknowledged that such stories contributed to their wariness to engage with technology. In their study of security-related stories, Rader, Wash, and Brooks [44] found that nearly all undergraduates in their sample said a story changed how they thought about security; half said it changed their behavior, and nearly half said they retold the story to others. Our study shows that security-related stories clearly resonate with low-SES families as well. This suggests that incorporating privacy- and security-related stories into such resources could help the digital literacy messages stick. The dearth of computer security resources focused on mobile privacy and security [43], the prevalence with which low-SES families rely on mobile-only connectivity, and the variety of threats our participants described experiencing suggest that this topic could be a good place to start.

6.2 Next Steps: Using Participatory Design to Develop Educational Modules for Librarians and Families

Our next step is to create tools or exercises that will help people better address online or mobile threats, risks, and scams. Our findings highlight that people who have limited digital skills and few people in their network to answer their technology-related questions may develop mental models and strategies that do not serve their privacy or security interests [3]. Prior research has shown that people tend to look for evidence that confirms what they already believe and trust what they already know (a phenomenon known as “confirmation bias”) [29], [30]. We seek to create tools that help people question their assumptions about internet and mobile technologies while still respecting their experiences. We believe that this can enhance their digital literacy and foster mental models and strategies that serve their privacy and security interests.

In late 2018, we will conduct a series of participatory design (PD) sessions with low-SES families in the same library branches. PD is an especially useful method when working with marginalized populations as it provides insights that might otherwise have been missed. As Titlestad et al. [60]:31] note, “A key PD principle is to bridge and blur the user-designer distinction from both directions, through mutual learning processes.” In this way, PD serves as a “third space” where “participants can combine diverse knowledge into new insights and plans for action” [33]:166]. We will use a PD method known as bonded design, whereby we will engage with participants as partners and informants to develop low-fidelity prototypes of tools and exercises [31]. Initially, we may begin with a self-reflection exercise in which participants draw or discuss their own mental models in response to a privacy-related scenario derived from anecdotes presented in this study. Teachers have used this instructional method to learn about their students’ understandings of a science concept and how students’ understandings evolve across time [13]; we believe it can be useful for with our participants as well.

We will iterate on the low-fidelity prototypes and go through additional rounds of bonded design prototyping until these tools are fully developed. We also intend to leverage the position of librarians as trusted information intermediaries by inviting them to help facilitate these design sessions and co-design the resources. We believe that this approach will result in resources that incorporate the perspectives of populations that have low digital literacy and that discuss privacy and security in a way that resonates with their experiences of technology.

In considering this stage of our research project, we have found a useful connection with research on public health interventions. Decades of public health practices have contributed to and been integrated with behavioral science theories that were established to guide the design of interventions. For example, the Health Belief Model (HBM) [50] was developed to help understand why people did or did not use services for preventing (e.g., influenza vaccines) and detecting diseases (e.g., mammography screening) as well as for mitigating risky behaviors (e.g., risky sexual behaviors and injury). HBM theorizes that people’s beliefs about whether they are at risk for a disease or health problem, and their perceptions of the benefits of taking action to avoid it, influence their readiness to take action [12]. The core constructs of HBM are:

1. Perceived susceptibility and perceived severity
2. Perceived benefits and perceived barriers
3. Cues to action
4. Self-efficacy (added more recently)

We plan to adapt these constructs to our project to promote behaviors that protect privacy and security within marginalized communities. As emphasized above, we argue there is no universal set of privacy and security behaviors for every person to follow; therefore, we aim to design resources with a well-defined context, audience, and outcome in mind. For example, one context found in our study could be to improve awareness and knowledge of security risks for older immigrants who experiment with social media but do not believe they will become victims of scams.

6.3 Limitations

We note some limitations in our study. First, as mentioned in the Related Work section, while we adopted Park’s [42] definition of digital literacy and Hargittai’s [17] definition of self-efficacy of knowledge of computer and web-skills for the framing of this study, we acknowledge that these definitions are time-, technology- and context-bound, and may not be inclusive of all the digital privacy and security skills that we examined in this study. In addition to using these definitions, our mapping of the absence and presence of digital privacy and security skills relied on our own interpretations and previous digital privacy and security research that were discussed in the Related Work section. Through an iterative coding process that allowed each of the authors to check and verify coded transcripts, we attempted to minimize any inaccurate or privileged interpretations.

Second, as noted in the Method section, we relied on the library branch demographics to determine participants’ socioeconomic status; this is an imprecise measure used to avoid awkward decisions about inclusion/exclusion of participants based on arbitrary cutoff points. However, we believe that partnering with library staff who knew our study’s research goals yielded participants who were well-positioned to contribute to this study.

Third, we collected self-reported data about participants’ attitudes, opinions, and behaviors. In some cases, participants may have been reluctant to share their experiences due to embarrassment (e.g., they did not want to be perceived as unintelligent) when talking with researchers from a university. Family dynamics could also have affected interviews, such as cases where a child may have been less willing to share their experiences in front of a parent, or an adult unwilling to talk about sensitive matters in front of their children.

Our PD work will address these limitations in part by engaging with participants as design informants and partners. By seeding the PD activities with a privacy-related scenario, rather than asking participants to design materials based on their direct experiences, we hope to ameliorate any feelings of embarrassment. We may also conduct separate PD sessions for children and parents to help each speak more freely about their experiences.

7 CONCLUSION

Research, assessment, and design projects often overlook the needs of marginalized groups, leading to technological solutions that do not account for the unique challenges and contexts within which those groups operate. In this paper, we began to address one such area where there has been a paucity of research: low-socioeconomic families and digital privacy and security. People from economically disadvantaged backgrounds face a variety of challenges, and it is essential for researchers to work with these individuals to understand how they make sense of technology broadly, and privacy and security risks specifically. By better understanding their mental models of privacy and security, researchers and designers can design tools both tailored to their specific needs and ones that will be adopted by the community.

In this study, we worked with four public libraries and one nonprofit Latino advocacy organization to connect us with people who could most benefit from training and resources to improve digital literacy and enhance their technological self-efficacy. These public spaces are especially useful for this kind of research because they are highly valued by local community members for the various free services they provide, and because federal agencies often direct people to visit libraries when they need assistance completing online forms for federal assistance.

Findings from this study reveal that the barriers to protecting personal information online are compounded by many factors, and privacy issues are far from straightforward. Often, the need to submit a form quickly overrides any concerns about who might see the information on that form—especially when a timely submission may determine when a utility bill is paid or groceries are purchased. Therefore, we propose a research and design approach that relies heavily on the methods embedded in participatory design, and specifically bonded design techniques, whereby low-SES participants act as key informants to the content and design of the educational materials. Such approaches have previously been effective in designing public health interventions, which also complex challenges areas about people's behavior [56].

Finally, we see this research space as offering many opportunities for the technology industry to partner with academia to develop meaningful interventions to improve digital literacy, narrow the digital literacy gap, and enhance privacy and security skills. We stress the focus on partnerships here because a clear finding from both the current research and prior studies has been that technology alone will not solve the challenges our participants described, and technology designed without a strong understanding of the unique needs and context that shape this population's use of technology will likely not be adopted. Therefore, we encourage companies to consider creating additional research opportunities specifically targeted at the privacy and security challenges that low-SES populations face and be willing to dedicate significant resources to incentivizing more researchers to work with, learn from, and assist these users in learning how to navigate online services safely and securely.

ACKNOWLEDGMENTS

This research is funded by an IMLS National Leadership Grant, LG-81-16-0154-16. We would like to thank Andrea Castillo for her help with data collection, particularly in conducting Spanish-language interviews with some participants. We would also like to 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.

A Appendix: Abbreviated Version of Codebook

Code Name	***Description/Definition***	***Examples***
Adult technology literacy	Descriptions of how comfortable the adult feels about performing tasks with the computer or descriptions by them of “what they know/don't know.” This includes comfort with technology.	*“I try to use it (computer) on the job. I have a chaplaincy position, and I wasn't technology-savvy, so I kind of lost the job.”*
Child technology literacy	Descriptions of how comfortable the child feel about performing tasks with the computer or descriptions by them of "what they know/don't know." This includes comfort with technology.	*“I feel comfortable because it's only one in the house feel comfortable searching up stuff for my grandma.”*
Child information intermediary	Descriptions of how the child helps the parent with information tasks (e.g., Google search, translating text).	*[Interviewer: How did you learn to use the computer and the internet?] “My daughter, the older one. She began using it at school, they taught her so she’s helped me.”*
Security threats/ scams	Experiences with online scams or threats to their personal information, not necessary of their own experience. Also when they're talking about experiences that could have been scams but they don't frame them as such.	*“I went on Facebook and I got booted out. Don't know how. It was like my computer, it went on Facebook, and then all of a sudden I got this virus… A pop-up ad that I went and I clicked on it and I had to change my whole Facebook.”*
Privacy definition	Interviewee’s definition of privacy. Descriptions about how they understand how privacy and security function.	*“Keeping all your things personal to yourself without nobody else knowing what it is.”*
Adult privacy concerns	Descriptions of parents’ online privacy concerns (or lack of) for themselves.	*“You can do all you can do and you could still get robbed or you could still get hurt or your privacy, your identity stolen, but as soon as they steal my identity, they wouldn't want it. They'd probably want to give it back.”*
Parent privacy concerns for kids	Concerns parents have about their children regarding technology use (e.g., stranger danger).	*“Yes, I worry. I tell my kids when they get on something that requires payment, I tell them to be very careful, to make sure it’s safe.”*

Adult privacy and security behaviors	Adults describing steps they take to control of their information online (e.g., buying from a trusted vendor, using only phone for certain transactions, changing privacy settings when creating an account). Also, descriptions of the heuristics they apply when using technology.	*"I don't put my information on Facebook. The only information that's on my Facebook is my user name, my email address and my password, my phone number for Messenger and all that."*
Child privacy concerns	Child describes his/her online privacy concerns (or lack thereof).	*"Sometimes I hear rumors that they can spy on us through WhatsApp. It's not very safe because there's hackers who can go into your account, so it can't be very safe."*
Child privacy behavior	Child describes how they take control of their online privacy (or lack of). Also, descriptions of heuristics the child applies when using technology.	*"I really don't post anything about my personal life [on Facebook]. I have a personal account that I use for school. I deleted every photo on it and I just kind of look at other people's accounts, that's what I use it for."*
Trust in librarians	Interviewee's trust or other perception of librarians	*"I wasn't thinking that she [the librarian] would steal my information because, in fact, when the computer turns off, it turns off everything so there's no way to reopen what you were working on, like your credit card number."*
Library technology services	Interviewee's experiences using technology services (computer, Internet) in a public library.	*"I like the free WiFi. I also come [to the library] so I don't use all my data at home, on my laptop, so I come here and use it."*
Desired resources and training	The resources and training on privacy and security the adults would like or envision receiving (both in response to specific prompt and examples mentioned throughout the interview).	*"An app would be the best way. I know a lot of people in my age group get most of our news from apps. I find out a lot of things like what's on the news from Snapchat and everything else. Oh I didn't know this happened, let me check Snapchat, see what happened. Oh this happened."*
Trust/Lack of Trust in Online Sources	Comments specifically describing how much an interviewee trusts/does not trust technology generally or specific companies/sites and why they feel this way. Also include code if they make comments about their general trust/lack of trust of people (but not librarians, as that is captured in the "Trust in Librarians" code).	*"I don't trust people."* *"I mean I'm just being honest. I trust no one."* *"The internet is ... I don't trust it."*
Technology Monitoring	Overseeing family tech use (e.g., parents making sure kids do age-appropriate activities). Examples could include checking browser history, requiring your kid be friends with you on social media, etc.	*"If he (son) wanted one (Facebook account), I'd be okay, because I'd be checking everything."*
Technology Rules & Advice	Rules for technology use as described by adults OR children. Advice that participants have given or received	*"My wife has it where when they log onto something she sees it. So even if I'm not over their shoulder looking, eventually she'll pull up her thing and she'll see if they're watching something they're not ... my youngest son, sometimes he is*

	about what to do/not do when using technology.	*watching things that maybe have violence in it or something that we don't agree with, we take it away, and he understands he shouldn't be watching it. He's usually pretty good about policing himself."*
Trust in children	Parents describing their trust/lack of trust of their kids when using technology.	*"Then I have to cut it down because he was really not keeping up with the school work. I said, I have to cut it down. So no, I don't do searches, but I trust that he's playing what he's playing with who he said he's playing."*

REFERENCES

[1] Annette Baier. 1986. Trust and antitrust. *Ethics, 96*, 2 (1986), 231-260.

[2] Jonathan Ben-Naim, Jean-François Bonnefon, Andreas Herzig, Sylvie Leblois and Emiliano Lorini. 2017. Computer-mediated trust in self-interested expert recommendations. *AI & Society, 25*, 4 (2010), 413-422. DOI: https://doi.org/10.1007/978-3-319-49115-8_12

[3] Denis Besnard, David Greathead and Gordon Baxter. 2004. When mental models go wrong: co-occurrences in dynamic, critical systems. *International Journal of Human-Computer Studies, 60,* 1 (2004), 117-128. DOI: https://doi.org/10.1016/j.ijhcs.2003.09.001

[4] Jasmine Bowers, Bradley Reaves, Imani N. Sherman, Patrick Traynor, and Kevin Butler. 2017. Regulators, mount up! Analysis of privacy policies for mobile money services. *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)* (pp. 97-114). USENIX Association.

[5] Jay Chen, Michael Paik, and Kelly McCabe. 2014. Exploring internet security perceptions and practices in urban Ghana. *Proceedings of the Symposium on Usable Privacy and Security (SOUPS*) (pp. 129-142). USENIX Association.

[6] Wei Chen and Simon Fong. 2010. Social network collaborative filtering framework and online trust factors: A case study on Facebook. *Proceedings of the Fifth International Conference on Digital Information Management (ICDIM)* (pp. 266-273). IEEE. DOI: https://doi.org/10.1109/ICDIM.2010.5664676

[7] Erika Chin, Adrienne Porter Felt, Vyas Sekar and David Wagner. 2012. Measuring user confidence in smartphone security and privacy. *Proceedings of the Eighth Symposium on Usable Privacy and Security* (Article No. 1). New York: ACM.

[8] Catherine Dwyer, Starr Hiltz and Katia Passerini. 2007. Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *AMCIS 2007 proceedings* (2007), Article 339.

[9] Matthew S Eastin and Robert LaRose. 2000. Internet self-efficacy and the psychology of the digital divide. *Journal of Computer-Mediated Communication, 6,* 1 (2000), n.p.

[10] Andrew J Flanagin and Miriam J Metzger. 2008. Digital media and youth: Unparalleled opportunity and unprecedented responsibility. *Digital Media, Youth, and Credibility,* Edited by Miriam J. Metzger and Andrew J. Flanagin. The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning. Cambridge, MA: The MIT Press, 2008 (pp. 5–28).

[11] Qin Gao, Ye Tian and Mengyuan Tu. 2015. Exploring factors influencing Chinese user's perceived credibility of health and safety information on Weibo. *Computers in Human Behavior, 45* (2015), 21-31. DOI: https://doi.org/10.1016/j.chb.2014.11.071

[12] Karen Glanz and Donald B. Bishop. 2010. The role of behavioral science theory in development and implementation of public health interventions. *Annual Review of Public Health, 31* (2010), 399-418. DOI: https://doi.org/10.1146/annurev.publhealth.012809.103604

[13] Shawn Glynn. 1997. Drawing mental models. *The Science Teacher, 64*, 1 (1997), 30-32.

[14] Ricardo Gomez and Elizabeth Gould. 2010. The "cool factor" of public access to ICT: Users' perceptions of trust in libraries, telecentres and cybercafés in developing countries. *Information Technology & People, 23*, 3 (2010), 247-264.

[15] Eszter Hargittai. 2002. Second-level digital divide: Mapping differences in people's online skills. *First Monday, 7*, 4 (2002), n.p.

[16] Eszter Hargittai. 2003. The digital divide and what to do about it. New economy handbook, 2003 (2003), 821-839.

[17] Eszter Hargittai. 2005. Survey measures of Web-oriented digital literacy. *Social Science Computer Review, 23* 3, (2005), 371-379. DOI:http://dx.doi.org/10.1177/0894439305275911

[18] Eszter Hargittai and Yuli Patrick Hsieh. 2012. Succinct survey measures of web-use skills. Social Science Computer Review, 30, 1 (2012), 95-107.

[19] Amanda Hess. 2017. How privacy became a commodity for the rich and powerful. *New York Times Magazine* (May 9, 2017).

[20] Donna L Hoffman, Thomas P Novak and Marcos Peralta. 1999. Building consumer trust online. *Communications of the ACM, 42*, 4 (1999), 80-85.

[21] John B Horrigan. 2016. *Digital readiness gaps*. Pew Research Center (2016).

[22] Adele E Howe, Indrajit Ray, Mark Roberts, Malgorzata Urbanska and Zinta Byrne. 2012. The psychology of security for the home computer user. Proceedings of the 2012 IEEE Symposium on Security and Privacy (pp. 209-223). IEEE. DOI: http://dx.doi.org/10.1109/SP.2012.23

[23] Internet Crime Complaint Center. 2016. Internet Crime Report Internet Crime Complaint Center. Available: https://pdf.ic3.gov/2016_IC3Report.pdf

[24] Iulia Ion, Rob Reeder and Sunny Consolvo. 2015. "... No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices. City.

[25] Paul T Jaeger, John Carlo Bertot, Kim M Thompson, Sarah M Katz and Elizabeth J DeCoster. 2012. The intersection of public policy and public access: Digital divides, digital literacy, digital inclusion, and public libraries. *Public Library Quarterly, 31,* 1 (2012), 1-20.

[26] Joseph W Jerome. 2013. Buying and selling privacy: Big data's difference burdens and benefits. *Stanfor. Law Review Online, 66* (2013), 47-53

[27] Kyung Kyu Kim and Bipin Prabhakar. 2004. Initial trust and the adoption of B2C e-commerce: The case of internet banking. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 35,* 2 (2004), 50-64.

[28] Kimberly Kindy. May 30, 2017. How Congress dismantled federal Internet privacy rules. *Washington Post.* Available: https://www.washingtonpost.com/politics/how-congress-dismantled-federal-internet-privacy-rules/2017/05/29/7ad06e14-2f5b-11e7-8674-437ddb6e813e_story.html?utm_term=.7de600dbda1c

[29] Joshua Klayman and Young-Won Ha. 1987. Confirmation, disconfirmation, and information in hypothesis testing. *Psychological Review, 94*, 2 (1987), 211-228.

[30] Joshua Klayman and Young-won Ha. 1989. Hypothesis testing in rule discovery: Strategy, structure, and content. *Journal of Experimental Psychology: Learning, Memory, and Cognition, 15,* 4 (1989), 596-604.

[31] Andrew Large, Valerie Nesset, Jamshid Beheshti and Leanne Bowler. 2006. "Bonded design": A novel approach to intergenerational information technology design. *Library & Information Science Research, 28,* 1 (2006), 64-82.

[32] Jialiu Lin, Shahriyar Amini, Jason I Hong, Norman Sadeh, Janne Lindqvist and Joy Zhang. 2012. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. *Proceedings of the 2012 ACM Conference on Ubiquitous Computing (UbiComp '12)* (pp. 501-510). New York: ACM. DOI: http://dx.doi.org/10.1145/2370216.2370290

[33] Yvonna S. Lincoln and Egon G. Guba. *Naturalistic inquiry*. Sage Publications, Beverly Hills, CA, 1985.

[34] Linlin Liu, Matthew KO Lee, Renjing Liu and Jiawen Chen. 2018. Trust transfer in social media brand communities: The role of consumer engagement. *International Journal of Information Management, 41* (2018), 1-13. DOI: https://doi.org/10.1016/j.ijinfomgt.2018.02.006

[35] Niklas Luhmann. 2000. Vertrauen: Ein mechanismus der reduktion sozialer komplexität. Grove/Atlantic, Inc.

[36] Michael Mackert, LeeAnn Kahlor, Diane Tyler and Jamie Gustafson. 2009. Designing e-health interventions for low-health-literate culturally diverse parents: addressing the obesity epidemic. *Telemedicine and e-Health, 15,* 7 (2009), 672-677. DOI: DOI: 10.1089/tmj.2009.0012

[37] Madden. 2017. Privacy, security, and digital inequality. Data & Society, https://datasociety.net/pubs/prv/DataAndSociety_PrivacySecurityandDigitalInequality.pdf

[38] Mary Madden, Michele Gilman, Karen Levy and Alice Marwick. 2017. Privacy, poverty, and big data: a matrix of vulnerabilities for poor Americans. *Wash. UL Rev., 95* (2017), 53-125.

[39] Michael Muller. 2009. *Participatory design: The third space in HCI.* Boca Raton, FL: CRC Press.

[40] New York Police Department. n.d. NYPD crime prevention alert: Beware of scams using Green Dot MoneyPak cards. Available: http://www.nyc.gov/html/nypd/downloads/pdf/crime_prevention/greendot.pdf

[41] Kenneth Olmstead and Aaron Smith. 2017. *Americans and cybersecurity.* Pew Research Center (2017).

[42] Yong Jin Park. 2013. Digital literacy and privacy behavior online. *Communication Research, 40 2* (2013), 215-236. DOI: 10.1177/0093650211418338

[43] Emilee Rader and Rick Wash. 2015. Identifying patterns in informal sources of security information. *Journal of Cybersecurity, 1,* 1 (2015), 121-144. DOI: https://doi.org/10.1093/cybsec/tyv008

[44] Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories as informal lessons about security. *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS) (*Article 6). New York: ACM, DOI: https://doi.org/10.1145/2335356.2335364

[45] Lee Rainie, Sara Kiesler, Ruogu Kang, Mary Madden, Maeve Duggan, Stephanie Brown and Laura Dabbish. 2013. *Anonymity, privacy, and security online.* Pew Research Center (2013). Available: http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/

[46] Elissa M Redmiles, Sean Kross and Michelle L Mazurek. 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* (pp. 931-936). New York: ACM. DOI: http://dx.doi.org/10.1145/3025453.3025673

[47] Dina Ribbink, Allard CR Van Riel, Veronica Liljander and Sandra Streukens. 2004. Comfort your online customer: quality, trust and loyalty on the internet. *Managing Service Quality: An International Journal, 14,* 6 (2004), 446-456.

[48] Ronald E Rice and James EKatz. 2003. Comparing internet and mobile phone usage: digital divides of usage, adoption, and dropouts. *Telecommunications Policy, 27, 8-9* (2006), 597-823. DOI: https://doi.org/10.1016/S0308-5961(03)00068-5

[49] Soo Young Rieh. 2010. Credibility and cognitive authority of information. In M. Bates & M. N. Maack (Eds.) *Encyclopedia of Library and Information Sciences, 3rd Ed.* (pp. 1337-1344), New York: Taylor and Francis Group, LLC. (2010).

[50] Irwin M Rosenstock, Victor J Strecher, and Marshall H Becker. 1988. Social learning theory and the health belief model. *Health Education Quarterly, 15 2,* (1988) 175–183. http://dx.doi.org/10.1177/109019818801500203

[51] Aaron Shaw and Eszter Hargittai. 2018. The pipeline of online participation inequalities: The case of Wikipedia editing. *Journal of Communication, 68* 1 (2018), 143-168. DOI: https://doi.org/10.1093/joc/jqx003

[52] Wanita Sherchan, Surya Nepal and Cecile Paris. 2013. A survey of trust in social networks. *ACM Computing Surveys (CSUR), 45,* 4 (2013), Article No. 47. DOI: 10.1145/2501654.2501661

[53] Michael Siegrist and George Cvetkovich. 2000. Perception of hazards: The role of social trust and knowledge. *Risk Analysis, 20*, 5 (2000), 713-720. DOI: https://doi.org/10.1111/0272-4332.205064

[54] Aaron Smith. 2017. *What the public knows about cybersecurity*. Pew Research Center on Internet and American Life (March 22, 2017). Available: http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/

[55] Laura D Stanley. 2003. Beyond access: psychosocial barriers to computer literacy special issue: ICTs and community networking. *The Information Society, 19,* 5 (2003), 407-416. DOI: https://doi.org/10.1080/715720560

[56] Bradley D Stein, Sheryl Kataoka, Lisa H Jaycox, Marleen Wong, Marleen, et al. 2002. Theoretical basis and program design of a school-based mental health intervention for traumatized Immigrant children: A collaborative research partnership. *The Journal of Behavioral Health Services & Research, 29,* 3 (2002), 318-326. DOI: https://doi.org/10.1007/BF02287371

[57] Mega Subramaniam, Natalie Greene Taylor, Beth St. Jean, Rebecca Follman, Christie Kodama and Dana Casciotti. 2015. As simple as that?: Tween credibility assessment in a complex online world. *Journal of Documentation, 71*, 3 (2015), 550-571. DOI: https://doi.org/10.1108/JD-03-2014-0049

[58] Paul Taylor, Cary Funk and April Clark. 2007. *Americans and social trust: Who, where and why.* Pew Research Center. (2007). Available: http://www.pewsocialtrends.org/2007/02/22/americans-and-social-trust-who-where-and-why/

[59] Kim M Thompson, Paul T Jaeger, Natalie Greene Taylor, Mega Subramaniam and John Carlo Bertot. 2014. *Digital literacy and digital inclusion: Information policy and the public library.* Rowman & Littlefield.

[60] Ola Hodne Titlestad, Knut Staring and Jørn Braa. 2009. Distributed development to enable user participation: Multilevel design in the HISP network. *Scandinavian Journal of Information Systems, 21,* 1 (2009), Article 3.

[61] Craig W Trumbo and Katherine A McComas. 2003. The function of credibility in information processing for risk perception. *Risk Analysis, 23,* 2 (2003), 343-353. DOI: https://doi.org/10.1111/1539-6924.00313

[62] Alexander van Deursen, Ellen Helsper, Rebecca Eynon and Jan van Dijk. 2017. The compoundness and sequentiality of digital inequality. *International Journal of Communication, 11* (2017), 452-473.

[63] Jan Van Dijk and Kenneth Hacker. 2003. The digital divide as a complex and dynamic phenomenon. The *Information Society, 19,* 4 (2003), 315-326. DOI: https://doi.org/10.1080/01972240309487

[64] Jan AGM Van Dijk. 2005. *The deepening divide: Inequality in the information society.* Sage Publications.

[65] Andreas Vårheim. 2011. Gracious space: Library programming strategies towards immigrants as tools in the creation of social capital. *Library & Information Science Research, 33,* 1 (2011), 12-18. DOI: https://doi.org/10.1016/j.lisr.2010.04.005

[66] Andreas Vårheim. 2014. Trust in libraries and trust in most people: Social capital creation in the public library. *The Library Quarterly, 84, 3* (2014), 258-277. DOI: https://doi.org/10.1086/676487

[67] Aditya Vashistha, Richard Anderson, and Shrirang Mare. 2018. Examining security and privacy research in developing regions. COMPASS '18: ACM SIGCAS Conference on Computing and Sustainable Societies (Article No. 25). Menlo Park and San Jose, CA, USA. ACM, New York. DOI: https://doi.org/10.1145/3209811.3209818

[68] Jessica Vitak, Yuting Liao, Priya Kumar and Mega Subramaniam. 2018. Librarians as Information Intermediaries: Navigating Tensions Between Being Helpful and Being Liable. *Proceedings of the 13th Annual iConference, Lecture Notes in Computer Science, vol 10766* (pp. 693-702). London: Springer.

[69] Jessica Vitak, Yuting Liao, Priya Kumar, Michael Zimmer, and Katie Kritikos. 2018. Privacy attitudes and data valuation among fitness tracker users. *Proceedings of the 13th Annual iConference, Lecture Notes in Computer Science, vol 10766* (pp. 229-239). London: Springer.

[70] Rick Wash. 2010. Folk models of home computer security. *Proceedings of the Sixth Symposium on Usable Privacy and Security* (Article No. 11). New York: ACM.

[71] Rick Wash and Emilee Rader. 2011. Influencing mental models of security: a research agenda. *Proceedings of the 2011 New Security Paradigms Workshop* (pp. 57-66). New York: ACM.

[72] Rick Wash and Emilee J Rader. 2015. Too much knowledge? security beliefs and protective behaviors among united states internet users. *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)* (pp. 309-325). Usenix Association.

Received April 2018; revised July 2018; accepted September 2018.