Cross-Contextual Examination of Older Adults' Privacy Concerns, Behaviors, and Vulnerabilities

Yixin Zou*
Max Planck Institute for Security and Privacy / University of Michigan

Kaiwen Sun
University of Michigan

Tanisha Afnan
University of Michigan

Ruba Abu-Salma
King's College London

Robin Brewer
University of Michigan

Florian Schaub
University of Michigan

ABSTRACT

A growing body of research has examined the privacy concerns and behaviors of older adults, often within specific contexts. It remains unclear to what extent older adults' privacy concerns and behaviors vary across contexts and whether old age is the primary factor influencing privacy vulnerabilities. To address this gap, we conducted semi-structured interviews with 43 older adults (aged 65 to 89) in the United States. Our interviews were grounded in five scenarios: account and device sharing, healthcare, online advertising, social networking, and cybercrime. Our cross-contextual analysis showed that cybercrime was a recurring and pressing concern across scenarios; privacy concerns and protective behaviors were rarely mentioned in the healthcare scenario. Across all scenarios, participants' threat models and strategies revolved around data collection rather than other stages in which privacy harms may occur; they employed various active strategies to safeguard their privacy while trusting service providers to protect their information. Our findings underscore the need to revisit the discussion around privacy vulnerability and aging. Vulnerability levels among our participants varied widely and were often influenced by factors beyond age, such as tech savviness and income. We discuss opportunities for privacy interventions, technologies, and education that promote positive aging and recognize diversity among older adults.

KEYWORDS

privacy, older adults, privacy concern, privacy behavior, privacy vulnerability.

1 INTRODUCTION

Older adults are increasingly adopting digital technologies and engaging in online activities [9], which introduce privacy and security threats. Prior research has positioned older adults as a vulnerable group [49, 55, 98, 153], susceptible to privacy violations that disproportionately affect their safety and well-being [89]. For example, older adults with declining health conditions may need health monitoring technologies for independent living while accepting continuous surveillance [37, 138]. Older adults with limited digital skills may resist tech use [49], limiting learning opportunities for privacy management and self-protection [24]. Caregivers and family members, despite good intentions, may engage in paternalistic "care surveillance" that impacts older adults' agency [18, 93, 94, 98].

People's privacy behavior is known to be context-dependent [2], with "context" referring to "various spheres of life [...] or conventional routines" according to the theory of contextual integrity [103]. Despite growing privacy research on older adults, most prior studies have explored the topic broadly [49, 52, 113] without making comparisons across different contexts. Some studies have delved into a specific context such as social media [111] or healthcare [15, 43, 67]. To address this gap, we employed a cross-contextual approach to assess the extent to which older adults' privacy concerns and behaviors are influenced by context. Specifically, we conducted a qualitative study with 43 older adults (aged 65 to 89) in the United States to explore their privacy concerns, behaviors, and vulnerabilities across five interview scenarios: account and device sharing, healthcare, online advertising, social networking, and cybercrime.

Our findings show that across all five scenarios, participants expressed concerns about falling victim to cybercrime (such as scams and fraudulent charges) consistently and often unprompted; they perceived themselves as more vulnerable to cybercrime than younger counterparts, a distinction that was rarely noted in other scenarios. In contrast, participants were rarely concerned about their health information within the healthcare scenario, prioritizing quality of care and health insurance over privacy. While prior work [49] has characterized older adults' threat models along Solove's four dimensions of privacy harm (data collection, processing, dissemination, and invasion) [128], our participants' concerns and protective behaviors across all scenarios primarily centered on data collection. Unlike prior work that highlighted older adults' reliance on passive mitigation strategies [49], our participants employed various active strategies (e.g., configuring privacy/authentication settings and selectively disclosing sensitive information) while trusting service providers to protect and uphold their privacy.

A key implication of our findings is that we need to expand the current discourse around privacy vulnerability. Our findings challenge the notion of older adults as a whole being a vulnerable group. Our participants believed that older and younger adults were equally at risk for most scenarios (except for cybercrime), and our analysis showed the actual vulnerability varied greatly among individuals—those with lower tech usage, digital literacy, and income experienced more concrete privacy harms. Some tech-savvy participants acted as guardians of their communities for

*Work primarily done as a Ph.D. student/postdoc at the University of Michigan.

Proceedings on Privacy Enhancing Technologies 2024(1), 133–150

https://doi.org/10.56553/popets-2024-0009

privacy protection, contradicting prior deficit-based narratives in characterizing older adults [49, 51, 135, 158, 164]. Our research provides empirical support for Anaraky and Knijnenburg's position paper that attributing privacy vulnerability solely to old age is an oversimplification [53]. We conclude with recommendations for designing privacy-protective interventions, technologies, and education that attend to the more positive aspects of the aging experience [74].

2 RELATED WORK

2.1 Privacy Vulnerability and Aging

Vulnerability is a key concept in HCI and human-centered privacy research, highlighting how technical systems can perpetuate sociopolitical and historical injustices [124]. However, the term has faced criticism for being disempowering and promoting stigmatization, especially in accessibility research [80]. In privacy research, older adults have been labeled as a vulnerable group [89, 121, 153]. The labeling is sometimes reinforced by deficit-based narratives in prior studies: older adults are "more susceptible to fraud" [51], "express lower concerns about information privacy" [158], or are "particularly vulnerable to certain risks and experience difficulties in mitigating them" [49] compared to younger adults or the general population. However, some scholars advocate for moving beyond age-related limitations and instead focusing on the wisdom and unique perspectives of older adults [74]; other scholars suggest the importance of disentangling age from other factors that may influence one's vulnerability [53].

One of these factors is *health*, as aging can lead to changes to one's sensory, physical and cognitive functioning [70, 159]. Older adults with (mild) cognitive impairments may struggle to recognize scams or fully consider the implications of sharing personal information [94]. Chronic disabling conditions may necessitate the use of health monitoring technologies to remain physically independent [50], and the adoption of such technologies introduces concerns about privacy and ethics [110]. Declining health conditions can amplify one's dependence on others such as family members, neighbors, and professional caregivers to oversee their privacy and tech use [49, 93, 94], leading to "care surveillance" [43]. In fact, fraud by a family member is a common form of elder financial abuse [65]. Even when caregivers initiate monitoring with good intentions, heavy-handed stewardship can limit older adults' agency and hinder their learning of digital threats and respective self-protection skills [98].

Digital literacy is another critical factor that should be separated from age. While younger and older adults may differ in their technology use, older adults are adopting new technologies [45] and engaging in various online activities [21, 22], making it important to examine their privacy behaviors across contexts. However, non-adoption of technology among older adults may occur due to cost considerations [36], inappropriate design [49], limited self-efficacy [6], low interest [32], and fears driven by ageist stereotypes [85]. Low levels of tech usage and digital literacy can subsequently limit one's privacy self-protection [24, 81, 139]. Our findings contribute to a growing body of research emphasizing the heterogeneity in older adults' tech use [61, 133] and how tech-savvy older adults often act as influencers and guardians of their peers [22, 75, 101, 102].

2.2 Older Adults' Concerns and Behaviors

We organize our literature review in line with the five scenarios explored in our interviews; below we note how our findings add to the existing literature for each scenario. We also examine prior research on age-based differences in privacy concerns and behaviors, as it relates to our findings around privacy vulnerability.

Account and device sharing. Sharing digital accounts and devices is a well-documented practice [154], observed among romantic partners [105] and in workplace settings [152]. Several studies highlight that older adults—especially those less tech-savvy [49], with physical or cognitive impairments [94], or living in collectivist cultures [98]—often give household members or professional caregivers access to their personal accounts and devices, and this practice could introduce tensions around privacy and autonomy.

Older adults may also share account/device access as a way of preparing for their digital legacy to be passed on to family members and friends after their passing. This practice of preparing digital data for death, however, has mostly been explored among younger populations [30, 57]. We studied account and device sharing by older adults considering they will need to face the prospect of death but may experience anxiety and uncertainty in planning [167]. We also included questions about public and second-hand devices to compare with Frik et al.'s study [49], in which older adult participants exhibited limited risk awareness and concerns in these cases.

Healthcare. Prior research has shown that older adults often find health monitoring technologies intrusive and constraining [43, 82], but tend to accept these technologies as an inevitable trade-off for safety, care, and aging in place [15, 71, 83]. Older adults generally express comfort with their health data being shared with doctors, caregivers, and family members but not with unknown parties [15, 19, 158], and they prefer data collection and sharing to occur only when necessary, such as in emergency situations [99].

We conducted our interviews during the COVID-19 pandemic. Beyond the direct health risks posed by COVID-19, the fear, stress, and loneliness from social isolation during the pandemic further affected older adults' health and well-being [108]. Our study provides updated insights into older adults' privacy concerns and behaviors related to healthcare, shaped by the COVID-19 pandemic. We also examined older adults' privacy considerations when using patient portals, a topic that has been studied [76, 119] but rarely with a specific focus on privacy.

Online advertising. Online advertising often targets individuals based on their online activities, personal information, and inferred interests [166]. Due to the complex and opaque nature of ad tracking practices [166], most consumers have limited knowledge regarding the extent to which advertisers can access their personal data [54, 58]. Consumers may also hold misconceptions [1, 162] such as conflating online tracking with malware [92]. While some people find targeted ads useful and relevant [144], others find them intrusive and discomforting [10, 44, 63]. Recent work has also investigated user perceptions of problematic, untrustworthy, or distasteful ads [165].

Notably, most studies in this area have centered on general adult or younger populations. Limited prior work involving older adults has indicated that they exhibit higher engagement with certain

types of advertising such as social video ads [86] while being skeptical about social media-based advertising [25], and older adults are especially likely to be shown problematic advertising (such as scams or clickbait) on Facebook [5]. We addressed this gap by exploring privacy issues of online advertising with older adults in depth, particularly with regard to their mental models and attitudes toward age-based advertising.

Social networking. Social media use among U.S. older adults continues to grow, but older adults still have lower usage than younger groups [45]. Privacy concerns can deter older adults from using social media, particularly when these concerns outweigh potential social benefits [73, 84, 100, 111, 150]. Some studies have found differences between older and younger adults [73, 84, 146]: older adults are more concerned about who can access their information [111], while younger generations, especially teens, are more concerned about context collapse or self-representation [35, 72].

Zoom and other videoconferencing tools also gained popularity during the COVID-19 pandemic for maintaining social contact [137]. Prior work on younger users' privacy attitudes toward remote communications has found that users lack autonomy in choosing conferencing tools and microphone/webcam use [41]. We examined older adults' privacy considerations towards videoconferencing tools and compared them to pre-pandemic findings on other social networking sites like Facebook, given the pandemic's impact on people's social behaviors [13].

Cybercrime. Bossler and Berenblum define cybercrime as "computer assisted crime" across four categories: cyber-trespass (e.g., unauthorized system access), cyber-theft (e.g., identity theft and online fraud), cyber-obscenity (e.g., child pornography), and cyberviolence (e.g., cyberstalking); they also note a lack of standardized legal definitions in this field [20]. Mainstream media often depict older adults as vulnerable to cybercrime, especially cyber-theft [46, 120]. However, findings from academic literature are mixed. Simons et al. find that older adults are disproportionately victimized by certain types of fraud, such as tech-support scams and impersonation [125]. Ross et al. argue that there is no compelling evidence of higher consumer fraud rates among older adults [118]. Several studies suggest that susceptibility to scams or phishing attacks can be influenced by other factors such as income [149] and gender [104].

Studies with older adults highlight that media portrayals heighten their anxiety about spam emails and scam calls [113]. Being defrauded impacts older adults' health and well-being irrespective of financial loss, as victims experience derision and censure [12]. In Frik et al.'s study [49], older adult participants held diverse views on their own vulnerabilities: some believed they were easy targets due to low technical literacy and lack of support, whereas others doubted that their information was valuable enough to be exploited. Unlike the prior subsections, cybercrime is primarily associated with risks and harms, whereas other contexts like healthcare also offer tangible benefits. We decided to include cybercrime as an interview scenario given its relevance to older adults and the ageist stereotypes around cybercrime, and we were particularly interested in uncovering more nuanced factors that contribute to older adults' self-perceived as well as actual vulnerability to cybercrime.

Age-based differences. Several studies have examined the privacy concerns and behaviors of older adults in North America [48, 49, 111, 112]: older adults' concerns centered on security issues (e.g., scams and identity theft) and institutional threats (e.g., data sold to third parties) rather than interpersonal privacy [112]; passive strategies (like limiting/avoiding technology use) were commonly employed, while active mitigation strategies were rarer and triggered only in response to privacy violations [49]. Older adults' privacy concerns and behaviors are also culturally dependent: studies in countries with collectivist cultures such as India [98] and China [123, 134] have highlighted older adults' privacy management as a collective practice, with household members overseeing older adults to ensure their safety.

While some prior research has characterized older adults as being generally vulnerable to privacy risks and violations, empirical findings on differences between older and younger adults are mixed. Some studies indicate that older adults are less likely to react to privacy risks [135, 164] and adopt fewer protective behaviors on social media [73]. Other research suggests that older adults are not necessarily worse at protecting themselves; rather, they have distinct concerns and priorities. For example, older adults often perceive higher risks in online banking and e-commerce [113] and are more likely to base privacy decisions on a privacy calculus [52]. Some studies have found no significant age differences in online privacy sensitivity and attention to privacy policies [66]. These inconsistent findings may be due to different studies examining different contexts and using constructs with different granularity (e.g., general attitudes vs. specific concerns) [3].

3 METHODS

To qualitatively explore the privacy experiences of older adults within and across various contexts, we conducted semi-structured interviews with 43 individuals (≥65 years) in the United States. The interviews took place between August and October 2021 and were conducted using a combination of video calls and in-person meetings based on participants' preferences. Our study materials (including the screening survey, interview protocol, and codebook) are available online for reference.[1]

3.1 Interview Protocol

Our interview protocol consisted of two main parts:

Part 1: We began by asking participants to describe their technology ownership and use. We then indirectly elicited participants' privacy-related concerns by asking whether they had issues with any technologies they used. If privacy concerns were not brought up, we probed further about what information they wanted to protect and who they perceived as potential threats. We designed the sequence in this way (reserving potentially priming privacy-related questions toward the end and only asking them if the participant had not raised these topics) to mitigate potential researcher bias and social desirability bias, following the practices in other work that also touched on sensitive and charged topics [117].

Part 2: We delved into participants' privacy perceptions and strategies in five scenarios. Scenarios are commonly used in HCI research to explore values and attitudes toward technology [7, 8, 161].

[1] https://osf.io/5mcve/?view_only=6c4ca8f9b0834c068642e37e14aab436

Our scenario selection was informed by our literature review in Section 2.2. All five scenarios are highly relevant to the daily lives of older adults, although findings specific to older adults and/or privacy varied. Specifically, prior work on account/device sharing and online advertising has predominantly focused on younger populations. Healthcare and social networking have more research specific to older adults, but most of it was conducted before the COVID-19 pandemic, which has impacted how people socialize and manage health issues [13]. Cybercrime is often laden with ageist stereotypes (assuming older adults are always more vulnerable), and we wanted to compare these stereotypes with the actual experiences and perceptions of older adults.

The interview procedure for all scenarios followed a similar structure: first broad questions about mental models and personal experiences, then questions about more specific concerns and protective strategies (if applicable). To assess participants' perceptions of age-related vulnerability, we asked "How do you feel about your possibility of experiencing X (a negative incident) compared to those older/younger?" with X tailored to each scenario. To ensure we did not impose preconceptions, we mirrored participants' language in follow-up questions and confirmed our understanding of their responses with them [140]. We randomized the scenario order for each participant to mitigate order effects and potential fatigue toward scenarios discussed later. We concluded the interview by soliciting suggestions from participants on how to support older adults in privacy self-protection.

3.2 Participant Recruitment and Demographics

Our target demographic consisted of individuals aged 65 or older residing in the United States, following the CDC's definition of older adults [145]. We used various channels to broaden our recruitment: three local senior centers, a participant pool for clinical & health research at University of Michigan,[2] another participant pool hosted by the Healthier Black Elders Center at Wayne State University,[3] and snowball sampling. The majority of our participants came from the university-hosted pools and senior centers; only three participants joined the study through snowball sampling.

We asked interested individuals to complete a screening survey, which was accessible in several formats (online, phone, and paper). We used the screening survey to verify the age criterion and to recruit a diverse sample across age, race, gender, and socioeconomic status. We did, however, exclude individuals with serious cognitive impairments since engaging with this population requires specific protocols that we were not able to implement [136]. We also excluded non-English speakers due to limitations in our research team's language capabilities.

We pre-tested our interview protocol with three pilot participants. Based on the pilot data, we made minor adjustments to the interview protocol and settled on an interview duration of 60-90 minutes to ensure comprehensive coverage of all scenarios without causing participant fatigue. For the main data collection, the first author conducted interviews with 43 participants. Most interviews were one-on-one; two sessions were done with couples who preferred to take the interview together. We kept interviewing participants until data saturation was reached. Interviews were conducted via phone, Zoom, or at one of the partnering senior centers depending on the participant's choice. The interviews lasted 82 minutes on average. A few participants took breaks during the interview, but none withdrew from the study or expressed concerns regarding the interview length. Each participant received a $30 check as compensation. With all participants' consent, interviews were recorded and later transcribed by a professional transcription service.

Table 1 in Appendix A provides details of participant demographics. Our 43 participants were 65-89 years old (mean: 72; median: 71) and approximately balanced in gender (19 men, 23 women, one no response). Participants exhibited diversity across income, race, and self-reported health conditions, but were more educated than the general U.S. population [142, 143]. The majority of participants lived in their own or rented homes and did not have caregivers. Seven participants used assistive devices such as wheelchairs, canes/walking sticks, and hearing aids.

For technology use, most participants were regular users of computers (41) and smartphones (34). More than half (26) also regularly used tablets. Multi-device usage was common: 24 used all three types of devices, and 15 used two. By comparison, smartphones were present in 84% of all U.S. households in 2018, followed by 78% for desktops/laptops and 63% for tablets [141], indicating that our participants' tech adoption mirrored that of the general population. Smart device adoption was relatively low in our sample: 11 used smart TVs, and seven used smart speakers or voice assistants.

3.3 Data Analysis

After transcribing and double-checking all interview transcripts, the first author went through all transcripts to create an initial codebook using a combination of deductive and inductive approaches: the codebook's overall structure was informed by the interview protocol and prior literature; specific codes were mostly paraphrases of what participants said.

To ensure the reliability and consistency of the coding process, the first and second authors independently coded one transcript each, then convened to compare codes, address discrepancies, and modify the codebook; this iterative process was repeated for six transcripts until the two researchers agreed on code saturation. The two authors then used the 'training' feature in Dedoose, a qualitative data analysis tool, to calculate inter-rater reliability before independent coding. The first author coded an additional 14 transcripts to ensure a reasonable coverage of each code. The second author then coded the same set of excerpts coded by the first author. The two researchers achieved Cohen's $\kappa = 0.74$ across all codes, indicating good inter-rater reliability. The two researchers then split the remaining 21 transcripts and coded them independently, and the first author applied the final codebook to the initial six transcripts for consistency. Other co-authors were involved in discussions about the codebook and preliminary findings through regular meetings.

Our final codebook consisted of 296 codes across six categories: one about general privacy concerns and behaviors and five for the respective scenarios. The codes in each category were grouped

[2] https://umhealthresearch.org
[3] https://mcuaaar.org/cores/community-liaison-and-recruitment-core/healthier-black-elders-center/

into consistent sub-categories to facilitate cross-scenario comparisons: general attitudes, specific concerns, challenges in addressing concerns, protective behaviors, and age-based differences.

As our study was qualitative, we focused on describing specific themes rather than making quantitative claims about themes [14]. Following practices in other qualitative work [17, 40, 59], we adopted the following terminology to provide a qualitative estimation of the frequency of themes: a few (0-20%), some (20-40%), about half (40-60%), many (60-80%), and almost all (80-100%).

3.4 Ethics

Our study was reviewed and determined exempt from oversight by the University of Michigan's Institutional Review Board. Following a community-based participatory approach [151], we engaged our participants and community partners throughout the research process for a mutually beneficial experience. For example, we asked staff at the senior centers to provide feedback on our draft interview protocol to ensure the questions were appropriate. We followed trauma-informed practices [28] in conducting the interviews, such as being an active and empathetic listener when participants shared their stories, and clearly communicating options of skipping a question or stopping the participation. As a way to give back to the community, we used our research insights to develop a workshop series on online self-defense and ran the workshops with our partnering senior centers. Thirteen of our interview participants attended the workshops; all spoke positively about the experience and the workshop topics' relevance to their concerns.

3.5 Limitations

While our qualitative approach allowed deep insights into participants' lived experiences, it has limitations. Some limitations pertain to the qualitative method and sampling practices. For example, we cannot claim that our sample is representative of all American older adults; our primary aim was not to achieve representativeness but rather to capture diverse perspectives. Our participants were diverse regarding income and race, but they were geographically concentrated and more educated than the broader U.S. population [142]. The sample characteristics may have resulted from our localized recruitment—we opted for this approach to build trust with our participants, reach individuals who might not be accessible through online recruitment, and expand the reach of our workshops. Because our study was conducted in the U.S., some of our findings might be specific to the country or region. One should be careful in generalizing these findings beyond the U.S., and our study opens opportunities for future replication studies in other countries with different cultural values and consumer protection frameworks.

Another limitation of our study relates to the interview scenarios, as cybercrime is more focused on risks and harm compared to other scenarios. Nonetheless, we decided to include cybercrime due to its high relevance to older adults' existing concerns and ageist stereotypes around this topic. While it is possible that discussions about cybercrime might have primed participants to bring up this topic in other scenarios, this was partially mitigated by randomizing the scenario order for each participant. We also observed that participants who received the cybercrime scenario late in their interviews often still spontaneously discussed it in earlier scenarios.

4 FINDINGS

We first discuss participants' threat models and privacy concerns in general (Section 4.1), followed by participants' concerns and behaviors for specific scenarios (Sections 4.2–4.5). We end by comparing findings across the five scenarios (Section 4.7).

4.1 General Threat Models

4.1.1 Heightened concerns about financial information. As the concept of "privacy" can be broad and abstract, we asked participants instead about the specific types of information they would like to protect. Financial information, such as bank account and credit card numbers, was mentioned by about half of the participants. Some also highlighted social security numbers, a unique personal identifier used in the United States. P34 discussed negative incidents that can result in financial loss as their top concerns:

> *I may not have any money. I may have an outstanding debt . . . My major concern is my identity being taken, and as a result of my identity being taken, my financial security has been compromised or has been taken away from me.*

However, privacy harms encompass more than just financial losses [31] when accounting for harms to reputation, psychological well-being, autonomy, discrimination, and more. These harms were less recognized by participants, as P3 said, *"Financial information is probably the most relevant thing. The rest of my life is pretty much an open book . . . Somebody sees that I go on a porn site. That's me."* P18 raised the point that leaked passwords could lead to the compromise of financial accounts: *"One of the big things that I worry about is somebody getting a hold of my passwords and user ID that would get them into info on my banking and other financial institutions."* P15 mentioned health information but indicated that it was secondary to financial information in terms of privacy concerns: *"I don't worry about the portal so much . . . I've already got my Medicare, and so far I can't be refused for having [my] problems . . . It's mostly financial."*

4.1.2 Cybercriminals as the major threat actor. In line with concerns about financial information, about half of our participants identified cybercriminals as the primary threat to their personal information. The specific terms they used included "hackers," "scammers," "spammers," "people trying to steal things," and "people operating from the dark web." Some participants shared personal encounters with scams and fraudulent charges. P1 recounted stories they had come across in the news:

> *There are lonely seniors. You'll hear some news about a guy . . . gets hacked . . . A somewhat younger pretty lady will connect with him, and be able to access his finances . . . So, my concern is mainly [about] if they hack and get my personal information because hackers are those intelligent criminals.*

A few participants identified tech companies as another threat actor, particularly Google/Alphabet and Meta. P13 discussed the extensive data collection and aggregation practices employed by these companies: *"Google captures . . . anytime you do any online shopping. That information is captured and shared between organizations. In aggregate, they can build up a pretty detailed profile view of what your interests are."* P12 expressed varying levels of trust

in different companies, indicating that not all tech companies are perceived as equal threats:

> *Microsoft, I'm not as worried about information being shared by them . . . not so much privacy. I would say anything involving the Alphabet as an organization . . . I have too many firsthand experiences that I've been uncomfortable with. Information is shared from one site to another without express consent. And I can't seem to find any features that I could turn on that prevent it . . . It's something personally I can't trust.*

Interestingly, no participant mentioned the government as a threat actor. In fact, a few indicated that they were not concerned about government surveillance due to their belief that they had nothing to hide—a prevalent yet flawed argument about privacy [129]—such as P1: *"I'm not a member of any political party or secret organization . . . I have no fear of the police, FBI, or any governmental agent."* This lack of concern about government stands in contrast to heightened concerns about government surveillance among other high-risk populations such as undocumented immigrants [56], migrant domestic workers [127], and Muslim-American women [4], likely because our participants' identities and backgrounds did not intersect much with these populations. Similarly, no participant identified their family members or caregivers as threat actors, despite them being a major threat vector for elder fraud [65].

4.1.3 Learning from community and commercial resources. Prior work involving U.K. older adults has identified social, community, and commercial resources, as well as broadcast and digital media, as major cybersecurity information resources [101]. Our participants mentioned all five as sources for learning about privacy self-defense, with community resources, commercial resources, and the media being more popular. Starting with community resources as a source of support, P22 highlighted senior center classes: *"The senior center had contacts with the lawyer, and he'd come in and just discuss [the credit freeze] . . . People would ask whatever question they had."* P41 identified the American Association of Retired Persons (AARP): *"They have print materials . . . Zoom classes . . . If you're a member, every month they'll send you a newsletter."*

Another source of support was commercial resources, including customer support services such as AppleCare and professional tech support. For instance, P28 subscribed to Geek Squad and highlighted the benefits of their periodic checkups: *"Once or twice a year, [we] have what they call a checkup where they just delete duplicate files . . . make sure you've updated all your programs, and you've installed everything you need."* While experts no longer recommend third-party antivirus software [96], some participants continued to use such software. P9 noted trust and brand loyalty as relevant factors: *"I've used Norton for so long . . . I have trusted them with whenever it comes up for renewal. I don't even question how they've been pricing."* The protections offered by third-party antivirus software may be excessive, but they did raise our participants' awareness of basic risks and encouraged positive behaviors, as in P27's case:

> *I have Malwarebytes, and I'm quite happy with that. I think they've done a fairly good job. . . . They have a newsletter every week, and it's quite informative . . . They often tell you that there's all this phishing going on, and to be very careful about opening some of these emails that look suspicious. And so I take them at that word, and I do just discard a lot of [emails] because they're obviously not legitimate.*

Prior work using deficit-based narratives has portrayed older adults as passive consumers of information [53] who find it challenging or unnecessary to learn about cybersecurity or privacy [98, 101]. Our findings present a more nuanced perspective, as some participants acted as educators and influencers within their communities. P32 acknowledged the respective challenges in doing this:

> *She will want me to order something through my account. . . . She got mad at me the other day because I said I'm not doing it . . . I have done it a few times for her. But I want her to [learn]. She doesn't want to be tech-savvy. I'm not tech-savvy, but I know . . . the only way to learn stuff is you might make a mistake.*

P19 and P38 helped run computer classes at their senior centers. P38 identified recurring challenges among their peers, including password management and using "BCC" when sending mass emails. P19 was concerned about the potential exclusion of less tech-savvy peers from educational programs:

> *I'm super literate with computers . . . There are a few people like me, but not many. And as they get older, they have a harder time using the technology that's available, but they need that technology even more . . . You're missing a whole segment of the bell curve. Those are people who simply don't come [to the classes]. They have home phones and they don't use cell phone technology, and they don't get emails.*

4.2 Account and Device Sharing

4.2.1 Sharing digital assets in preparation for death or accidents. Half of our participants mentioned sharing passwords, mostly with family members and occasionally with close friends. Prior research has identified convenience and trust building as key drivers for password sharing among younger adults [126, 157], and our participants gave similar reasons. For example, P13 shared streaming service credentials with their son; P33 shared "everything" with their partner after decades of marriage.

However, most participants' primary motivation for sharing was preparation for unforeseen circumstances such as death or emergencies. For example, P18 shared, *"My mom and my sister have my social security number and my passwords . . . I trust [them] implicitly, and I feel better too because you'll never know."* For similar reasons, some participants also shared access to their financial accounts with family members and occasionally with a financial advisor or attorney. P8 made efforts to facilitate transparent communication between multiple parties:

> *I take care of all my own finances. My lawyer knows where all my accounts are. And . . . my adopted son is my advocate, and he's also my executor. So he knows . . . But he also knows where my lawyer is. And my lawyer knows where he is if something should happen.*

When we asked about post-death preparation for digital assets, some participants had already made plans. Others like P7, however,

only recognized the importance of this consideration in response to our probing:

> *If I were in a car accident and died, nobody would be able to get into my accounts, which will be bad. It would be weeks of sending mail and death certificates and wedding documents to prove that my wife is my heir and beneficiary. So I should do that. I'll put that on my list of things sometime.*

4.2.2 Struggles with password management. During discussions on account sharing, participants often highlighted password management as a recurring challenge. In contrast to studies involving younger populations [87, 106], our participants relied more on physical methods for password management: about half mentioned physically writing passwords down, and a few attempted to rely solely on their memory. No participant felt their current password management strategies were optimal; for instance, those who wrote passwords down would still have concerns over the "single point of failure" if their password notebook were to be stolen. While remembering all passwords is generally demanding, P30 emphasized age-related memory decline as a specific concern:

> *For important things like my banking, I want to keep going with the same one. I can't . . . They want a different one than you've used in the last 10 years. I can't remember 10 years' worth. What I do worry about, actually, is as I get older it's going to become harder and harder to do all that to keep track of it all.*

Only a few participants, typically those with a technical background, mentioned using password managers in their browsers and operating systems. The adoption rate of password managers was much lower in comparison to studies involving younger adults [87, 106]. Echoing prior work [114], P20 shared that non-adoption was due to distrust in cloud services storing their passwords:

> *I do not use any of the password apps where they say you can put in all your passwords, and it'll be secure, I just don't trust it. In my opinion, all of these systems were created by a person, and there's always a way . . . somebody else can figure out how to get into it.*

4.2.3 Risk Awareness of Public and Second-Hand Devices. A particular case of device sharing is public devices and Wi-Fi networks, which carry the risks of data leakage and Wi-Fi spoofing. This use case holds particular relevance for older adults given their lower ownership of personal computers or smartphones [9] while having communal places like senior centers that enable device sharing. Many participants reported using public computers and Wi-Fi networks in libraries, hotels, and shops.

In contrast to the findings in Frik et al.'s study [49], in which few participants expressed concerns about public devices and Wi-Fi networks, our participants (even with similar demographics) exhibited a heightened awareness of these risks. Although they could not always pinpoint specific negative events, they could recognize situations with increased risk. For example, P23 commented, *"I think it's easier to compromise my information [when using public devices]. I think people can get into them more easily."* About half of our participants mentioned that they consciously avoided sensitive activities such as banking when using public devices or Wi-Fi networks. P19 compared banking with other types of online activities regarding their sensitivity:

> *If somebody wants to hack into my gaming group and screw with my pictures . . . that's not going to kill me. So I don't really particularly care about that as much, but I stay away from banks and things that are high security. When we're traveling, oftentimes I'm looking up what attractions are there? What time does the museum open? . . . things that are not security-driven.*

A few participants also cleared their browsing history on exit when using a public computer. P32 shared how they developed this habit after someone compromised their social media account when it remained signed in:

> *Some years ago I did not sign out on Facebook [at libraries]. And so whoever came [next], they put a whole bunch of crazy stuff up there. And so my son called me up, 'Ma, was it really [you]?' 'Where were you at?' I said, 'I was at the library.' . . . So he deleted [my post] . . . Now I make sure I sign out if I'm on a public device.*

The exchange of second-hand devices can also lead to data leaks [16]. Some participants like P6 worried about unwiped data: *"When you get second-hand phones, they're contaminated . . . It's not good to buy used phones unless they've been cleaned or wiped."* Additionally, participants felt a lack of confidence in securely decommissioning their old devices, particularly when selling or donating to strangers, and desired more guidance. As P16 said, *"I have two laptops . . . just ready to go to the recycling, but I have to get the stuff off of them . . . I probably will pay to have somebody do it because I don't know what I'm doing."*

4.3 Healthcare

Our findings within the healthcare context mostly centered on patient portals and smartwatches, as they were adopted by almost all and some participants, respectively. A few participants also mentioned using health-tracking apps, step counters, and blood pressure monitors.

4.3.1 Trust in healthcare providers and smartwatch manufacturers. While a few participants expressed privacy concerns about their health information (see Section 4.1), about half of our participants shared that they trusted service providers (e.g., hospitals and smartwatch manufacturers) to securely handle their health information. This trust contrasts with the healthcare industry being one of the most common victims of data breaches [107] and instances of data exchange between healthcare providers and social media companies for commercial purposes [47]. Participants' trust in confidential information exchange with healthcare providers could be a result of social norms and existing laws, notably the Health Insurance Portability and Accountability Act (HIPAA), as P25 said: *"Any doctor that I'm dealing with can go to my portal and look up what other doctors have done or said . . . It's already in there. I don't feel that that's being shared inappropriately."*

Interestingly, P25 extended the same level of trust to smartwatch manufacturers, despite these entities being subject to different regulatory frameworks, and wearable devices having limited protection

under HIPAA: *"My Fitbit … it's like a watch … as far as I know, there are no data to take. It's just something I'm looking at … for my information only."* P12 explained that their trust in smartwatch manufacturers came from their own positive experiences and social influence:

> *You know that the Apple Health app … I have not personally heard of any episode where that recorded information was used [in]appropriately … I encountered a person in a focus group … where they were trying out the Apple Watch and recording various aspects of it. That person felt comfortable … and that was significant for me. I am not looking and would not be comfortable with any other entity.*

4.3.2 Concerns about breaches and health-based discrimination. Although participants generally expressed trust in health devices and portals, some voiced concerns about the potential compromise of their health information in data breaches when prompted, as P41 said: *"You kind of hear all the time where these health organizations are hacked … That's a big concern, and that's real."* P9 also noted concerns about health information being used for identity theft: *"Somebody can get a hold of a copy of your driver's license and your health care card and piece together enough to use it for some other purpose."* In addition, some participants expressed concerns about the potential use of their health information for advertising and insurance purposes. These concerns often overlapped with concerns regarding discrimination based on health or age, as P5 articulated:

> *It seems to me that the misuse of health information is not within the healthcare world … it's in the application, the decision-making of lenders and hirers … that would look at a health condition and determine that it's an additional risk … That's the abuse of the healthcare information that I'm concerned about.*

Nonetheless, only a few participants mentioned specific protective behaviors in response to their concerns. Examples include monitoring financial statements (following a healthcare breach notification) and removing prescription labels from medication bottles (to avoid medical identity theft). Overall, participants discussed much fewer privacy-protective behaviors (in terms of both diversity and frequency) in the healthcare scenario than in other scenarios.

4.4 Online advertising

4.4.1 Negative attitudes toward targeted advertising. Almost all participants had experiences with targeted ads, and many participants held negative sentiments. About half expressed frustration with the overwhelming volume of annoying targeted advertisements. P10 voiced concern about the surveillance capitalism model [171] that fuels targeted advertising: *"Every time I look at an ad, somebody knows that. And they put that data in a file somewhere that's linked to me somehow … They're going to sell that information to the manufacturer or the marketer … That's bothersome."* Other participants like P17 suspected that advertisers invaded their privacy by eavesdropping on their conversations, a common misconception [11] perpetuated by inadequate ad explanations [156]: *"My son bought a patio wood-burning oven pizza maker [called] Ooni … We were over to his house … talking a lot about the Ooni … I get home, and I look at Facebook, and I'm being sold Ooni pizza ovens."*

Consistent with prior work on the general public's mixed feelings regarding targeted advertising [144], a few participants did find targeted advertising useful and relevant. As P38 said, *"I think targeting ads helps people … I like knowing about something that I may not have known about that fits my situation."* Furthermore, some participants held relatively neutral views as they simply did not pay attention to ads or believed that their personal opinions were not easily influenced by ads. Our findings also align with prior work on consumers' challenges in understanding the full landscape of online advertising [38, 42, 156, 162]: when asked about the types of information possibly used for delivering targeted ads, about half of our participants exclusively mentioned site activities (e.g., browsing and search histories). Our participants mainly gave examples of targeted ads in the context of cross-website tracking, showing limited awareness of other individual and demographic factors used in ad targeting [166]; only a few discussed factors like age, race, ZIP code, and IP address.

Experiences with deceptive and discriminatory advertising. About half of our participants recounted experiences with "bad ads" [165] particularly deceptive ads, i.e., the claims and appearances could be misleading and different from consumers' actual experiences. P17, for example, recounted an emotionally manipulative ad:

> *It was this little plastic gadget … that supposedly some teenage boy with autism had invented … And I have a special place for people with disabilities … I see this on Facebook … Totally sell me with the story. My charge card is out … And it comes, and it's a piece of crap … And I realized, "Oh, you dummy. You fell prey. You were such an easy target because of the autistic kid.*

Regarding advertising specifically targeting older adults, our participants identified ads on Medicare, assistive technology, and funerary services as examples. While a few participants found age-based targeting positive (as it made ads more relevant) or neutral (equating it with other targeting categories like gender), some participants like P21 found the practice discriminatory and harmful for reinforcing ageist stereotypes: *"It's annoying because it just reminds you that you're older."* In addition, P30 was concerned about older adults' vulnerability to ad scams, showing that concerns over cybercrime carried over in this scenario:

> *The older we get, the less astute we are in paying attention to what this really means. That puts a lot of people at risk. We've heard about how many people can lose their money, not necessarily scammed but buying something we really have no use for. I guess they're free to advertise to anybody. I just don't like it.*

4.4.2 Protective strategies exist, but rendered ineffective. Some participants adopted an avoidance strategy when dealing with annoying or problematic ads, which typically involved ignoring them or removing them from their online feeds. This approach was particularly common among participants who held positive or neutral views about ads, as P11 explained, *"All you have to do is click on the X … hide the ad … ignore it. And if there are too many ads and it annoys you, then you don't go to those sites."*

However, avoidance-focused strategies do not fundamentally stop the excessive volume of ads. Some participants mentioned clicking on 'unsubscribe' in marketing emails but encountered challenges, as they either could not find the link or had to wait for a long time before they stopped receiving unwanted emails. Adding to prior work on users' folk models of online advertising and privacy settings [59, 77, 162], a few participants like P3 expressed distrust in the 'unsubscribe' feature, suspecting that clicking on it would trigger malware or even more spams:

> *I am concerned that you can generate more dissemination of information . . . that I wouldn't want people to have . . . [I] can't always trust that the unsubscribe location is really going to the service that I want to unsubscribe from . . . If it's a hacker . . . they're gonna take the information . . . and hack you some more.*

These ineffective strategies may explain why many participants felt they had limited control over what advertisers knew about them. As P4 described, their level of control was *"probably none, except just avoiding."* A few participants like P3 believed they had some control, but these participants were relatively experienced in using ad settings: *"There's always a setting somewhere that can be adjusted . . . It is left up to me to explore and see."* P22 was the only participant who felt they had a good amount of control, although their perception was narrowly based on the information they disclosed rather than inferences made by advertisers: *"I don't put a lot out there. I think that certainly gives me an edge on not getting advertising I don't need or don't want."*

4.5 Social Networking

While many participants used Facebook and Zoom, about half primarily connected with others via phone calls and text messages. A few participants mentioned other channels including emails, Instagram, Messenger, Twitter, and WhatsApp.

4.5.1 Benefit-risk analysis for adoption and use. Similar to findings in prior work [84, 100, 111], our participants deliberated the benefits versus risks/costs associated with specific social media platforms. While the benefits of staying connected and acquiring information apply to all age groups, they became more pronounced among our participants during the COVID-19 pandemic, which exacerbated feelings of social isolation and loneliness [60]. As such, P12 described their "calculated risk" for social media use: *"The very fact that I have to use YouTube to do certain functions puts me at risk, and it's a calculated risk . . . But we're so isolated as it is . . . It is unhealthy not to know what's going on in the world."*

Interestingly, in contrast to prior research [84, 111], our participants' major concerns with regard to using social media—before we specifically probed into privacy—revolved around disturbing or controversial content and dis/misinformation. In terms of privacy-related concerns, P36 mentioned possibilities of context collapse: *"If you use social media extensively, you are bound to have problems like misinterpretation . . . someone taking your post out of context."* P13 disliked the monetization of user data, a recurring concern that also appeared in the online advertising scenario: *"Facebook is notorious for sharing information and also establishing a profile . . . I don't want to make Mark Zuckerberg any richer."*

A few participants further voiced concerns about scams on social media: scams are already a recurring theme in the cybercrime scenario, but social media can amplify the reach of scams. P8, for example, shared their experience with romance scams: *"I have some weird guy that sent me [pictures] . . . He sent the same picture to my daughter-in-law . . . It's really a jungle out there."* Navigating scams and harassment was even more challenging for low-tech, low-income participants [149], as in the case of P6:

> *One day I got 1,000 friend requests [on Messenger] . . . but I accepted them all onto my page. Then I realized . . . I'm getting all these telephone calls [from] people trying to swagger me . . . They would call me up at two . . . in the morning and say, 'Hi, handsome. How are you?'*

4.5.2 Limited risk perceptions of Zoom. Zoom, a videoconferencing service, experienced a substantial surge in its user base during the COVID-19 pandemic [137]. Half of our participants mentioned adopting Zoom during the pandemic to maintain social, informational, and educational needs. A few shared concerns about Zoombombing [39, 79], and P9 even experienced it firsthand: *"There [was] this particular conversation that the council is having. And dirty pictures popped up. And then they had to shut down the Zoom thing."*

Nonetheless, participants who had heard of Zoombombing but had not experienced it personally expressed limited concerns, as they believed they would not be targeted. P36 shared, *"I don't think we will attract the attention of the criminals. . . . It's only the doctor and myself. So what is there to bomb? You want [to] bomb into a Zoom with 20 CEOs and the president of the United States."* Similarly, P7 speculated that Zoom would not engage in excessive data collection due to its business model: *"Why would they record a meeting amongst a family of four? They're not going to be able to monetize that."* However, Zoom has faced controversy for making false claims about end-to-end encryption while engaging in data exchanges with Facebook for monetization purposes [64]. These problematic data practices rarely influenced our participants' usage and trust in the platform. A few participants like P14 further mentioned relying on Zoom and its partner institutions for data protection: *"You heard so much about Zoom over the last two years that you figure, well, it's got to be a reasonable company. Hopefully, they have security measures in place."*

4.5.3 Skills and confidence in self-protection. In response to their concerns, participants actively employed protective strategies rather than relying on passive measures. P11 mentioned the option to limit their profile visibility: *"You can restrict your profile pretty well. So I do. You can't see my friends."* P28 described being careful about sharing sensitive information: *"I normally don't post it while we're away. I wouldn't want to advertise to the world that we're going to be out of town for a week."* P2 would block or unfriend someone in the case of scams or interpersonal conflicts: *"If I find people that are offensive . . . I will stop following them."* Some participants also adjusted their Zoom settings, such as muting themselves as needed and using a virtual background, similar to findings from prior work with younger populations [41]. Most of these proactive strategies reflected our participants' efficacy in navigating regular privacy settings on social media.

As in the online advertising scenario, participants' perceived level of control over their information on social media was closely tied to their confidence in configuring privacy settings. Many participants felt they had some control. Some participants like P39 even noted they had total control, though the perception was—similar to that in the online advertising scenario—primarily based on their knowledge of what they proactively shared rather than the inferences and data exchanges behind the scenes: *"I'm in control of what I put out there . . . If you put out everything, you expect to have some fallout . . . I don't put out personal stuff."*

4.6 Cybercrime

4.6.1 Concerns and negative experiences with scams and fraudulent charges. While prior work has identified cybercrime as a growing problem for older adults [97], our findings reveal older adults' concerns about specific types of cybercrime, both prompted and unprompted. When asked about their initial impressions of the term 'cybercrime,' some participants mentioned hacking attempts targeting government agencies and companies while others focused on cybercrime targeting individuals. For example, P21 was concerned about account compromises leading to financial loss: *"I do have some concerns about somebody stealing . . . not just your bank account, but your investments."* P42 highlighted concerns about scams: *"I think about a lot of the scam emails that I've been getting."*

About half of our participants reported receiving scam calls or phishing emails, with the majority successfully avoiding falling victim to them. Out of the 43 participants, only three had experienced unrecoverable financial losses. One potential factor contributing to participants' increased susceptibility to exploitation is concurrent financial hardship, as P32 recalled their experiences:

> *I was getting these text messages . . . to be like a mystery shopper . . . I received a check for about $1,500 . . . So I went to the bank . . . showed them the check. . . . And I was broke. And then she [bank manager] told me that it was a scam . . . That is how they get you because you'd be thinking about the money [when you're broke].*

Participants' vulnerability to scam attempts also relates to their level of digital literacy. P26, who considered themselves "computer illiterate," suspected their identity was stolen without recognizing that it was a social security scam: *"I got a call from the government that said somebody in Texas is using my social security number to extrapolate the funds out of bank . . . Maybe I have been a victim."* Nevertheless, having a technical background did not guarantee immunity to scams either, as in the case of P43, who ran a computer supply company but once lost $150 to a ransomware scam:

> *We had our computer locked up by a software company . . . They sold us a software package for $150 that would guarantee that we would not have our system locked up. And when I called the Geek Squad . . . they said all we had to do was just click on the control, alt, delete, and that would have restored us.*

4.6.2 Perceived higher vulnerability among older adults. Since prior literature [26, 97, 163] and news media [46, 120] have portrayed older adults as susceptible targets of cybercrime, we asked participants about their perceptions of age-related vulnerability to cybercrime. About half of the participants believed that older adults were more vulnerable and identified factors that could contribute to higher vulnerability, noting that older adults *"are naive with respect to technology"* (low tech-savviness), *"believe everything that they see"* (too trusting), and *"are more susceptible to [scammers] working on our emotions, like the grandparent scam . . . Seniors are lonely and just want somebody to talk to"* (subject to emotional manipulation). Interestingly, participants often used "they" when referring to older adults and rarely considered their own vulnerability. For instance, P33 were confident in their own resistance to cybercrime but expressed concern for others: *"I don't see why anybody would want to go after me . . . I'm not really worried about myself . . . There are a lot of [older] people that don't know or get scammed. That worries me."*

While older adults being more vulnerable to cybercrime is the dominant view, some participants believed that vulnerability to cybercrime is independent of age. P19, for instance, attributed cybercrime vulnerability to individual information-sharing habits: *"If you're careful and you don't expose yourself, I think you're going to be safer than if you just put your information out there willy-nilly."* Interestingly, a few participants considered younger adults more vulnerable due to more careless online behavior. As P14 said, *"The younger people spend so much time on their devices . . . They're savvy . . . but sometimes, you just think these people are not paying attention to what kind of danger they're putting themselves in."*

4.6.3 Adopting protective strategies. Participants shared a variety of strategies to protect themselves against cybercrime; the most prominent ones were frequent monitoring of financial accounts, avoiding phone calls (from unfamiliar numbers or in general), and looking for common indicators of phishing attempts (e.g., checking the sender's email address). These strategies aligned with established expert advice for online safety [116] and did not require advanced tech expertise. A strategy unique to older adults was relying on their crystallized intelligence, i.e., knowledge and skills acquired throughout life [168] as opposed to younger adults' fluid intelligence. In participants' own words, they relied on "common sense" they had developed over decades, as described by P35:

> *When someone comes to me asking questions about something I said that I did not put out to the public . . . that's a big red flag and an automatic delete . . . Because I'm older and already have . . . a whole bag of tricks from these many years of living that I can immediately use to evaluate and delete.*

Participants' ability to recognize scams could also come from their professional background. P28, for instance, had worked for the Internal Revenue Service and was able to quickly react to tax scams:

> *"I once got a call from someone who said they were from IRS and they said . . . if we didn't make a payment, there would be a warrant out for our arrest. I said, 'Well, I work for IRS and I know you're not from IRS. So I think you better stop what you're doing.' . . . And I hung up and report it."*

Participants also described acquiring protective strategies through firsthand encounters with scams, echoing prior work on security advice and behavior [115, 170]. For example, P31 shared:

> *The guy said that he was working for Amazon . . . He was able to put [a charge] back into my account . . . But in the meantime, I noticed that . . . when he took control, he started going into different information . . . And then something dawned on me. I said, 'Well, wait a minute. Why are you going through all these steps?' . . . A red flag would be when they start asking you for your financial information. I learned that now, because after this investigation, I was told by my financial institution never [to] give out your financial information.*

However, participants' strategies were not foolproof and sometimes led to unnecessary inconveniences or resignations. P26, for example, changed their phone number to avoid excessive spam calls, unaware of alternative strategies like blocking specific numbers or registering on the national Do Not Call list that do not entail the disruption of phone number changes [88]. P20 shared their reliance on service providers such as credit card companies and identity theft monitoring vendors for handling scams rather than self-protection: *"I would trust that the credit card company would tell me . . . Other than they tell me, throw that card away . . . we'll send you a new one, I don't think there's anything I personally can do."*

4.7 Cross-Contextual Insights

Having presented findings for each scenario, we now discuss common themes, similarities, and differences across scenarios.

4.7.1 Heightened and cross-scenario concerns about cybercrime. Our findings highlight cybercrime as a prominent and recurring concern for our participants across scenarios. In the initial general discussions on privacy (see Section 4.1), cybercriminals already emerged as the primary threat actors. Participants' definitions and concerns regarding cybercrime revolved around scams, fraud, phishing attacks, fraudulent charges, and identity theft. These definitions largely align with Bossler and Berenblum's categorization [20], focusing on two out of their four categories—cyber-trespass and cyber-theft. Importantly, we observed that cybercrime concerns and experiences were pervasive across scenarios, as participants discussed concerns about identity theft fueled by health information, being victimized by ad fraud, and encountering scams/harassment on social media, even before we probed about cybercrime.

In terms of vulnerability, we also found that cybercrime was the only scenario where a substantial portion of participants perceived higher vulnerability within their own age group compared to younger generations. Although participants rarely viewed themselves as more vulnerable than others—a possible manifestation of optimism bias [122]—they often expressed concerns for other individuals in their age group or older. Conversely, in the other scenarios, almost all participants believed that vulnerability was equally distributed across age groups and identified various factors contributing to heightened vulnerability irrespective of age. For instance, P10 identified health conditions and patient portal use as factors contributing to health-related privacy risks: *"I do have medical issues, I'm in and out of the patient portal more than a lot of people . . . I think the more you use a system, the higher the risk of being compromised."* P11 emphasized the importance of education level in dealing with problematic advertising: *"Somebody with less education might be distracted by these ads, whatever their age is. . . . Have you learned to research? Have you learned critical thinking? . . . Just don't follow what people tell you."*

4.7.2 Limited concerns and options for protecting health information. Our participants expressed the least privacy concerns in the healthcare scenario. Unlike in other scenarios, where participants readily identified threat actors and specific concerns without prompting, participants generally did not talk about healthcare-related privacy issues until prompted. This might be attributed to the relatively inconspicuous nature of health information misuse, particularly when discrimination is involved. None of our participants had personally experienced medical fraud or any associated financial losses. Our participants' perceptions may also have been shaped by news media—a common information resource—which provides limited coverage of security and privacy events in the healthcare industry [34].

In contrast to the diverse array of protective strategies observed in other scenarios, participants shared fewer strategies for safeguarding their health information. However, this limited action should not be equated with a lack of diligence. As aging-related health issues arise, older adults may have more frequent doctor's visits, naturally cultivating trust in their healthcare providers [27, 68]. While people may switch to a different service provider after negative privacy experiences like a data breach, most patients reasonably make decisions based on cost, coverage, and quality of care when selecting healthcare providers [147]. The "notice and choice" framework for protecting individual privacy has long been criticized for placing the burden of self-protection on consumers [130], and the shortcomings become even more problematic in the healthcare sector as consumers often have limited or virtually no choice.

4.7.3 Concerns and behaviors centered on information collection. Solove's taxonomy of privacy classifies privacy harms into four stages: information collection, information processing, information dissemination, and invasion [128]. Frik et al.'s study also characterized older adults' threat models along these four stages [49]. Nevertheless, our participants' primary concerns and strategies mostly centered on the information collection stage. For instance, some participants discussed limiting content/profile visibility in the social networking scenario and avoiding interactions with ads in the online advertising scenario. In both cases, participants' perceived control was tied to the amount of information they explicitly shared with other users and service providers. They felt more in control knowing they did not "put much out there." Only a few tech-savvy participants (e.g., P10 and P12) shared concerns about how companies aggregated and drew inferences from collected data. Very few participants mentioned concerns about information dissemination, except in the case of health-based discrimination, in which disclosing sensitive health information could jeopardize their health benefits.

4.7.4 Trust in service providers. Participants' trust in various service providers was a recurring theme across scenarios: trusting banks and credit card companies for detecting and resolving fraudulent charges, trusting healthcare providers and wearable device manufacturers for safeguarding health information, and trusting Zoom and partner institutions for ensuring the security of videoconferencing data. This trust is shaped by positive experiences

with service providers, unawareness regarding certain threats, and limited options for self-protection. Prior work has shown older adults' trust in healthcare professionals [23, 68] and preference for discussing health in-depth with a person rather than non-human sources [27]. In contrast, our findings suggest that older adults' trust extends beyond interpersonal contacts to encompass healthcare-related sociotechnical platforms, such as patient portals and video-conferencing tools facilitating virtual doctor's appointments.

Trust in service providers, particularly in the healthcare scenario due to the health needs of older adults, can be reasonable. However, there exists a risk that excessive trust leads to delegation or even abandonment of useful protective strategies. For instance, one might have limited control over how information in their health portal is used, but they can take retroactive measures when a breach happens. In contrast, with regard to cybercrime, many alternative measures can be taken to actively combat threats, such as using secure mobile payments to limit card fraud [132] and placing credit freezes to mitigate credit fraud [169], rather than relying solely on protections provided by financial institutions.

5 DISCUSSION

5.1 Comparisons with Prior Work

Consistent with prior work [112], our participants raised security-related concerns, such as scams and identity theft, even when we explicitly asked about online privacy. This suggests that our participants perceive security and privacy as interchangeable concepts, aligning with other work that highlights the diversity in privacy definitions and potential discrepancies between expert and end-user conceptions [33, 131]. In contrast to prior studies that emphasized older adults' reliance on passive mitigation strategies [49], our participants employed various active coping strategies, such as configuring privacy/authentication settings and exercising caution when disclosing sensitive information.

Our findings also affirm and extend prior research conducted within individual scenarios. For instance, older adults' privacy concerns and behaviors on social media have been well-researched. Our findings align with prior work [111] on common protective strategies, but our study also uncovered novel insights triggered by the COVID-19 pandemic as participants shared their adoption of Zoom and other videoconferencing tools. Our participants were adept at navigating corresponding privacy settings and expressed higher trust in service providers compared to more traditional social media platforms such as Facebook.

Contrary to prior research, our participants exhibited more risk awareness when using public and second-hand devices than those in Frik et al.'s study [49]. Additionally, in contrast to previous studies that highlighted older adults' negative perceptions of health monitoring technologies [15, 37, 71, 83], our participants expressed limited privacy concerns about their health information. However, it is important to contextualize this finding within our sample, as most of our participants lived independently and were not using technologies traditionally considered invasive such as in-home activity sensors and always-on web cameras [18].

While our study did not quantitatively compare privacy vulnerability between older and younger adults by recruiting both populations—making our findings less comparable to prior work that has done so [52, 73, 113]—our findings add more nuances to the deficit-based narratives of older adults [49, 51, 135, 158, 164] as our participants' vulnerability varied and could not be simply attributed to age. This divergence could come from our sample, as we recruited participants locally and some participants recruited via senior centers might have learned about privacy self-protections there. However, it is also likely that our cross-contextual interview approach and specific probing into participants' self-perceived vulnerability contributed to the new and different findings, as we unpack in Sections 5.2 and 5.3.

5.2 Contextual Effects of Privacy Concerns

Prior work, like Acquisti et al., emphasizes the role of context in understanding privacy concerns: "Individuals can, depending on the situation, exhibit anything ranging from extreme concern to apathy about privacy" [2]. Nissenbaum's theory of contextual integrity [103] similarly posits that societal norms shaping people's perceptions of what is private versus public vary across contexts. Our findings support the importance of context to some extent, as evidenced by concerns that are unique to certain scenarios, such as health-based discrimination in healthcare and password compromises in account/device sharing. Nevertheless, we also observe that privacy concerns are not entirely context-dependent as certain concerns transcend contexts. Specifically, cybercrime was a pressing concern among our participants, as they shared related concerns not only in the cybercrime scenario but also in healthcare, online advertising, and social networking scenarios. Another cross-contextual concern is related to surveillance capitalism [171] which was mentioned in both the online advertising and social networking scenarios, as participants expressed discomfort with the widespread collection and monetization of personal data by advertisers and social media platforms.

These findings underscore the need for further research to both qualitatively and quantitatively differentiate privacy concerns at the population, context, or individual level. For example, our findings already illuminate some population-level differences qualitatively: none of our participants identified the government as a threat actor, in contrast to other high-risk populations who hold heightened concerns about government surveillance [4, 56, 127]. Other research has also contributed to this direction quantitatively, such as Herbert et al.'s work that compares the digital security experiences of four at-risk groups (including older adults) [62] and Xu et al.'s context-contingent theory that explicates the mechanisms through which contexts influence privacy concerns and behaviors [160]. Notably, we observe that even within the same context, participants' concerns and vulnerabilities varied substantially and were shaped by many individual factors beyond age, as we discuss below.

5.3 Rethinking Privacy Vulnerability and Aging

In light of the growing research on specific populations who experience disproportionate privacy harms [89, 121], it is important to consider the nuanced differences between marginalization and vulnerability. According to Liang et al. [78], marginalization indicates a failing of society as marginalized individuals are being underserved, underrepresented, or forgotten, whereas vulnerability

may carry the connotation that the person is weak, in need of help, and burdensome [148, 155].

We argue that this distinction between marginalization and vulnerability is crucial in research with older adults. Our findings show the specific ways in which older adults experience marginalization. For example, P27 shared how they struggled with technologies not designed for their needs: *"The worst thing for me is manipulating that tiny [phone] keyboard . . . I have to use a stylus, with a little rubber on the end of it . . . because I just can't cope with that little keyboard."* P12 witnessed marginalization among their peers and expressed concerns: *"There are some [people] that do not join into our Zoom calls because they are afraid of the technology or they can't afford the technology. And they are completely left out."* Negative media portrayals can exacerbate feelings of marginalization and take an emotional toll on older adults themselves [12, 46, 85, 120]. This is also supported by our findings related to cybercrime: even though very few participants experienced direct repercussions, such as unrecoverable financial losses, many shared recurring concerns and stress, often accompanied by demanding behaviors (e.g., checking financial accounts frequently and avoiding phone calls) that come with emotional labor.

Nevertheless, our research challenges the prevailing vulnerability framing of older adults with multiple layers of supporting findings. First, a few participants who were well-versed in both privacy and technology played a crucial role in supporting and influencing their peers—this suggests that broadly labeling older adults as a vulnerable group is an oversimplification. Second, almost all participants believed that older and younger adults faced equal risks of privacy violations in most scenarios; even in the case of cybercrime, which triggered the most concerns among our participants, opinions were mixed. Third, participants' quotes and our analysis reveal that factors such as education, income, tech use, and online information disclosure influence one's privacy vulnerability more prominently than age. While these factors may correlate with age, they more often operate independently of age. For cybercrime, participants with a stronger resistance drew the knowledge from their work background, crystallized intelligence, and prior negative experiences; participants with more challenges navigating cybercrime tended to be those with concurrent financial hardship or low tech-savviness, although being tech-savvy does not guarantee immunity to scams either.

These findings highlight the need for more comprehensive frameworks that synthesize and quantify the various factors contributing to one's privacy vulnerability. Particularly for older adults, our findings provide empirical support to Knowles et al.'s plea to "seek design inspiration in narratives of positive aging" [74]. This philosophy presents numerous avenues for designing privacy interventions, technologies, and education for everyone growing old, as older adults are a highly heterogeneous population with unique traits that enable interesting research and design opportunities.

5.4 Technical and Educational Implications

Our findings open up several directions for future work on privacy-enhancing technologies. For example, our participants were motivated to share accounts and devices in anticipation of death and emergencies. However, some participants only became aware of this need after probing, and others were uncertain about the practical aspects of execution. We see opportunities to develop tools that support the data preparation for death [29] specifically for older adults. Drawing from our findings and prior work on safety settings for older adults with memory concerns [90, 91], such tools should enable multiple users to engage in socio-technical negotiations about agency and power (especially involving financial interests) and alleviate the anxiety that older adults may experience when contemplating their own mortality [167].

Besides building new tools, our research contributes insights into improving existing tools tailored to older adults' preferences while addressing misconceptions. In the account and device sharing scenario, our participants often struggled to safely decommission old devices. Participants were more familiar with physical means of destroying a device completely, while knowing but not trusting features like a factory reset. To make a factory reset more useful and explainable, digital devices could implement more granular settings in line with the user's goal (e.g., recycling, trading in, selling, donating it to friends or strangers) as well as more personalized advice (e.g., recommending reputable sites in the area based on the user's location). In another scenario, online advertising, some participants found age-based targeted ads discriminatory or offensive. To address such concerns, platforms should allow users to curate a list of topics they wish to avoid in ad targeting—a suggestion also made by prior work [28, 69]. While some platforms already provide adjustments for specific topics like alcohol, parenting, and politics [95], we see the need for co-designing ad filtering features with older adults who can provide unique insights into topics that may perpetuate ageist views.

Lastly, our findings highlight the need to support older adults in learning about privacy self-defense through educational efforts. Our participants suggested specific topics for education such as password management, privacy settings, the utility of protection services (e.g., antivirus and identity theft monitoring), and device decommissioning. In developing our online self-defense workshop materials, we incorporated these topics while mirroring our participants' mental models and language choices (e.g., disregarding the nuanced differences between security and privacy topics, and using 'hackers' to refer to malicious actors broadly). Going forward, there are opportunities to integrate this training into broader efforts of helping older adults build digital literacy skills such as workshops on 'how to use smartphones' or 'how to find jobs online.' Our findings suggest that community and commercial resources are reasonable starting points for deploying such training, and it might be useful to join forces with existing initiatives such as Apple's iPhone classes for older adults [109]. Our findings also suggest that older adults may turn to peers who are influencers and guardians—roles that a few of our participants already played—rather than acquiring new knowledge on their own. As such, a core part of training should be supporting older adults in developing self-learning and information-seeking skills, so that educational efforts are sustainable and can generate influence at scale.

ACKNOWLEDGMENTS

We are grateful to our participants for their time and invaluable insights. We extend our thanks to Ann Arbor Senior Center, Chelsea

Senior Center, Saline Area Senior Center, the Healthier Black Elders Center (HBEC), and UMHealthResearch for their crucial support in our research and participant recruitment efforts. HBEC was supported by a grant from the National Institutes of Health, 5P30 AG015281, and the Michigan Center for Urban African American Aging Research. We would like to thank Sam Ankenbaur, Xinru Tang, and the anonymous reviewers for their constructive feedback on previous drafts of this work.

This research has been partially supported by the Defense Advanced Research Projects Agency (DARPA) under grant No. HR0011 2010010. Kaiwen Sun has been supported by a Meta Research Ph.D. Fellowship. The content of the information does not necessarily reflect the position or the policy of the U.S. Government, and no official endorsement should be inferred. Approved for public release; distribution is unlimited.

REFERENCES

[1] Ruba Abu-Salma and Benjamin Livshits. 2020. Evaluating the end-user experience of private browsing mode. In *ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 313:1–313:12. https://doi.org/10.1145/3313831.3376440

[2] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2015. Privacy and human behavior in the age of information. *Science* 347, 6221 (2015), 509–514. https://doi.org/10.1126/science.aaa1465

[3] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2020. Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology* 30, 4 (2020), 736–758. https://doi.org/10.1002/jcpy.1191

[4] Tanisha Afnan, Yixin Zou, Maryam Mustafa, Mustafa Naseem, and Florian Schaub. 2022. Aunties, Strangers, and the FBI: Online Privacy Concerns and Experiences of Muslim-American Women. In *Symposium on Usable Security and Privacy (SOUPS)*. USENIX Association, Berkeley, CA, USA, 387–406. https://www.usenix.org/system/files/soups2022-afnan.pdf.

[5] Muhammad Ali, Angelica Goetzen, Alan Mislove, Elissa M Redmiles, and Piotr Sapiezynski. 2023. Problematic Advertising and its Disparate Exposure on Facebook. In *USENIX Security Symposium*. USENIX Association, Berkeley, CA, USA, 5665–5682. https://www.usenix.org/system/files/usenixsecurity23-ali.pdf.

[6] Hilde Alvseike and Kolbjørn Brønnick. 2012. Feasibility of the iPad as a hub for smart house technology in the elderly; effects of cognition, self-efficacy, and technology experience. *Journal of Multidisciplinary Healthcare* 5 (2012), 299–306. https://doi.org/10.2147/JMDH.S35344

[7] Tawfiq Ammari, Sarita Schoenebeck, and Meredith Morris. 2014. Accessing social support and overcoming judgment on social media among parents of children with special needs. *International AAAI Conference on Web and Social Media (ICWSM)* 8, 1 (2014), 22–31. https://ojs.aaai.org/index.php/ICWSM/article/view/14503/14352.

[8] Nazanin Andalibi and Justin Buss. 2020. The Human in Emotion Recognition on Social Media: Attitudes, Outcomes, Risks. In *ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 551:1–551:16. https://doi.org/10.1145/3313831.3376680

[9] Monica Anderson and Andrew Perrin. 2017. *Technology use among seniors*. Technical Report. Pew Research Center. https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2017/05/PI_2017.05.17_Older-Americans-Tech_FINAL.pdf.

[10] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. 2019. *Americans and privacy: Concerned, confused and feeling lack of control over their personal information*. Technical Report. Pew Research Center. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[11] AVG. 2019. Is Facebook Listening to Us Through Our Phones? https://www.avg.com/en/signal/facebook-listening-private-conversations. Accessed: 2023-02-28.

[12] Jan Bailey, Louise Taylor, Paul Kingston, and Geoffrey Watts. 2021. Older adults and "scams": evidence from the Mass Observation Archive. *The Journal of Adult Protection* 23, 1 (2021), 57–69. https://doi.org/10.1108/JAP-07-2020-0030

[13] Huanyu Bao, Bolin Cao, Yuan Xiong, Weiming Tang, et al. 2020. Digital media's role in the COVID-19 pandemic. *JMIR mHealth and uHealth* 8, 9 (2020), e20156.

[14] Martin W Bauer and George Gaskell. 2000. *Qualitative researching with text, image and sound: A practical handbook for social research*. Sage, London, England.

[15] Scott Beach, Richard Schulz, Julie Downs, Judith Matthews, Bruce Barron, and Katherine Seelman. 2009. Disability, age, and informational privacy attitudes in quality of life technology applications: Results from a national web survey. *ACM Transactions on Accessible Computing* 2, 1 (2009), 5:1–5:21. https://doi.org/10.1145/1525840.1525846

[16] Oussama BenRhouma, Ali AlZahrani, Ahmad AlKhodre, Abdallah Namoun, and Wasim Ahmad Bhat. 2022. To sell, or not to sell: social media data-breach in second-hand Android devices. *Information & Computer Security* 30, 1 (2022), 117–136. https://doi.org/10.1108/ICS-03-2021-0038

[17] Julia Bernd, Ruba Abu-Salma, Junghyun Choy, and Alisa Frik. 2022. Balancing Power Dynamics in Smart Homes: Nannies' Perspectives on How Cameras Reflect and Affect Relationships. In *Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, Berkeley, CA, USA, 687–706. https://www.usenix.org/system/files/soups2022-bernd.pdf.

[18] Clara Berridge and Terrie Fox Wetle. 2020. Why older adults and their children disagree about in-home surveillance technology, sensors, and tracking. *The Gerontologist* 60, 5 (2020), 926–934. https://doi.org/10.1093/geront/gnz068

[19] Linda Boise, Katherine Wild, Nora Mattek, Mary Ruhl, Hiroko H Dodge, and Jeffrey Kaye. 2013. Willingness of older adults to share data and privacy concerns after exposure to unobtrusive in-home monitoring. *Gerontechnology* 11, 3 (2013), 428–435. https://doi.org/10.4017/gt.2013.11.3.001.00

[20] Adam M Bossler and Tamar Berenblum. 2019. Introduction: new directions in cybercrime research. *Journal of Crime and Justice* 42, 5 (2019), 495–499. https://doi.org/10.1080/0735648X.2019.1692426

[21] Robin Brewer, Meredith Ringel Morris, and Anne Marie Piper. 2016. "Why would anybody do this?" Understanding Older Adults' Motivations and Challenges in Crowd Work. In *ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 2246–2257. https://doi.org/10.1145/2858036.2858198

[22] Robin Brewer and Anne Marie Piper. 2016. "Tell It Like It Really Is" A Case of Online Content Creation and Sharing Among Older Adult Bloggers. In *ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 5529–5542. https://doi.org/10.1145/2858036.2858379

[23] Charlotte Brooks, Claire Ballinger, Don Nutbeam, and Jo Adams. 2017. The importance of building trust and tailoring interactions when meeting older adults' health literacy needs. *Disability and rehabilitation* 39, 23 (2017), 2428–2435. https://doi.org/10.1080/09638288.2016.1231849

[24] Moritz Büchi, Natascha Just, and Michael Latzer. 2017. Caring is not enough: the importance of Internet skills for online privacy protection. *Information, Communication & Society* 20, 8 (2017), 1261–1278. https://doi.org/10.1080/1369118X.2016.1229001

[25] Hien Thu Bui. 2022. Exploring and explaining older consumers' behaviour in the boom of social media. *International Journal of Consumer Studies* 46, 2 (2022), 601–620. https://doi.org/10.1111/ijcs.12715

[26] Alexandra Burton, Claudia Cooper, Ayesha Dar, Lucy Mathews, and Kartikeya Tripathi. 2021. Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review. *Experimental gerontology* 159 (2021), 111678. https://doi.org/10.1016/j.exger.2021.111678

[27] Shomir Chaudhuri, Thai Le, Cathy White, Hilaire Thompson, and George Demiris. 2013. Examining health information–seeking behaviors of older adults. *Computers, informatics, nursing* 31, 11 (2013), 547–553. https://doi.org/10.1097/01.NCN.0000432131.92020.42

[28] Janet X Chen, Allison McDonald, Yixin Zou, Emily Tseng, Kevin A Roundy, Acar Tamersoy, Florian Schaub, Thomas Ristenpart, and Nicola Dell. 2022. Trauma-informed computing: Towards safer technology experiences for all. In *ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 544:1–544:20. https://doi.org/10.1145/3491102.3517475

[29] Janet X Chen, Francesco Vitale, and Joanna McGrenere. 2021. What Happens After Death? Using a Design Workbook to Understand User Expectations for Preparing Their Data. In *ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 169:1–169:13. https://doi.org/10.1145/3411764.3445359

[30] Liang-Kung Chen. 2020. Older adults and COVID-19 pandemic: Resilience matters. *Archives of Gerontology and Geriatrics* 89 (2020), 104124. https://doi.org/10.1016/j.archger.2020.104124

[31] Danielle Keats Citron and Daniel J Solove. 2022. Privacy harms. *Boston University Law Review* 102 (2022), 793–864. https://heinonline.org/HOL/Page?handle=hein.journals/bulr102&div=20&collection=journals.

[32] Jiska Cohen-Mansfield and James Biddison. 2007. The scope and future trends of gerontechnology: consumers' opinions and literature survey. *Journal of Technology in Human Services* 25, 3 (2007), 1–19. https://doi.org/10.1300/J017v25n03_01

[33] Jessica Colnago, Lorrie Faith Cranor, and Alessandro Acquisti. 2023. Is there a reverse privacy paradox? an exploratory analysis of gaps between privacy perspectives and privacy-seeking behaviors. *Proceedings on Privacy Enhancing Technologies* 1 (2023), 455–476. https://doi.org/10.56553/popets-2023-0027

[34] Sauvik Das, Joanne Lo, Laura Dabbish, and Jason I Hong. 2018. Breaking! A typology of security and privacy news and how it's shared. In *ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 1:1–1:12. https://doi.org/10.1145/3173574.3173575

[35] Ralf De Wolf. 2020. Contextualizing how teens manage personal and interpersonal privacy on social media. *New Media & Society* 22, 6 (2020), 1058–1075.

https://doi.org/10.1177/1461444819876570
[36] Julie A Delello and Rochell R McWhorter. 2017. Reducing the digital divide: Connecting older adults to iPad technology. *Journal of Applied Gerontology* 36, 1 (2017), 3–28. https://doi.org/10.1177/0733464815589985
[37] George Demiris, Debra Parker Oliver, Geraldine Dickey, Marjorie Skubic, and Marilyn Rantz. 2008. Findings from a participatory evaluation of a smart home application for older adults. *Technology and health care* 16, 2 (2008), 111–118. https://doi.org/10.3233/thc-2008-16205
[38] Claire Dolin, Ben Weinshel, Shawn Shan, Chang Min Hahn, Euirim Choi, Michelle L Mazurek, and Blase Ur. 2018. Unpacking perceptions of data-driven inferences underlying online targeting and personalization. In *ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 493:1–493:12. https://doi.org/10.1145/3173574.3174067
[39] Greg Elmer, Stephen J Neville, Anthony Burton, and Sabrina Ward-Kimola. 2021. Zoombombing during a global pandemic. *Social Media+ Society* 7, 3 (2021), 20563051211035356.
[40] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring How Privacy and Security Factor Into IoT Device Purchase Behavior. In *ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 534:1–534:12. https://doi.org/10.1145/3290605.3300764
[41] Pardis Emami-Naeini, Tiona Francisco, Tadayoshi Kohno, and Franziska Roesner. 2021. Understanding privacy attitudes and concerns towards remote communications during the COVID-19 pandemic. In *Symposium on Usable Security and Privacy (SOUPS)*. USENIX Association, Berkeley, CA, USA, 695–714. https://www.usenix.org/system/files/soups2021-emami-naeini.pdf.
[42] Motahhare Eslami, Sneha R Krishna Kumaran, Christian Sandvig, and Karrie Karahalios. 2018. Communicating algorithmic process in online behavioral advertising. In *ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 432:1–432:13. https://doi.org/10.1145/3173574.3174006
[43] Anna Essén. 2008. The two facets of electronic care surveillance: an exploration of the views of older people who live with monitoring devices. *Social science & medicine* 67, 1 (2008), 128–136. https://doi.org/10.1016/j.socscimed.2008.03.005
[44] Lisa Farman, Maria Leonora Comello, and Jeffrey R Edwards. 2020. Are consumers put off by retargeted ads on social media? Evidence for perceptions of marketing surveillance and decreased ad effectiveness. *Journal of Broadcasting & Electronic Media* 64, 2 (2020), 298–319. https://doi.org/10.1080/08838151.2020.1767292
[45] Michelle Faverio. 2022. *Share of those 65 and older who are tech users has grown in the past decade.* Technical Report. Pew Research Center. https://www.pewresearch.org/fact-tank/2022/01/13/share-of-those-65-and-older-who-are-tech-users-has-grown-in-the-past-decade/.
[46] Kate Fazzini. 2019. Here's how online scammers prey on older Americans, and what they should know to fight backElder fraud is real. Tell your parents, grandparents, and friends about these scams. https://www.cnbc.com/2019/11/23/new-research-pinpoints-how-elderly-people-are-targeted-in-online-scams.html. Accessed: 2023-02-28.
[47] Todd Feathers, Simon Fondrie-Teitler, Angie Waller, and Surya Mattu. 2022. Facebook Is Receiving Sensitive Medical Information from Hospital Websites. https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites. Accessed: 2023-02-28.
[48] Alisa Frik, Julia Bernd, Noura Alomar, and Serge Egelman. 2020. A qualitative model of older adults' contextual decision-making about information sharing. In *Workshop on the Economics of Information Security (WEIS)*. WEIS, online, 1–62. https://weis2020.econinfosec.org/wp-content/uploads/sites/8/2020/06/weis20-final42.pdf.
[49] Alisa Frik, Leysan Nurgalieva, Julia Bernd, Joyce Lee, Florian Schaub, and Serge Egelman. 2019. Privacy and security threat models and mitigation strategies of older adults. In *Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, Berkeley, CA, USA, 21–40. https://www.usenix.org/system/files/soups2019-frik.pdf.
[50] Vincenza Frisardi and Bruno P Imbimbo. 2011. Gerontechnology for demented patients: smart homes for smart aging. *Journal of Alzheimer's disease* 23, 1 (2011), 143–146. https://doi.org/10.3233/JAD-2010-101599
[51] Vaibhav Garg, Lesa Lorenzen-Huber, L Jean Camp, and Kay Connelly. 2012. Risk communication design for older adults. In *International Symposium on Automation and Robotics in Construction*, Vol. 29. Elsevier, Amsterdam, the Netherlands, 1–8. https://doi.org/10.22260/isarc2012/0030
[52] Reza Ghaiumy Anaraky, Kaileigh Angela Byrne, Pamela J Wisniewski, Xinru Page, and Bart Knijnenburg. 2021. To disclose or not to disclose: examining the privacy decision-making processes of older vs. younger adults. In *ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 686:1–686:14. https://doi.org/10.1145/3411764.3445204
[53] Reza Ghaiumy Anaraky and Bart Knijnenburg. 2021. A Research Agenda for Studying Young and Older Adults' Privacy Decisions. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3873573. Accessed: 2023-02-28.
[54] Cami Goray and Sarita Schoenebeck. 2022. Youths' Perceptions of Data Collection in Online Advertising and Social Media. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (2022), 475:1–475:27. https://doi.org/10.1145/3555576
[55] Galen A Grimes, Michelle G Hough, Elizabeth Mazur, and Margaret L Signorella. 2010. Older adults' knowledge of internet hazards. *Educational Gerontology* 36, 3 (2010), 173–192. https://doi.org/10.1080/03601270903183065
[56] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H Mhaidli, Kentaro Toyama, and Florian Schaub. 2018. Keeping a low profile? Technology, risk and privacy among undocumented immigrants. In *ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 114:1–114:15. https://doi.org/10.1145/3173574.3173688
[57] Rebecca Gulotta, William Odom, Haakon Faste, and Jodi Forlizzi. 2014. Legacy in the age of the internet: reflections on how interactive systems shape how we are remembered. In *ACM Conference on Designing Interactive Systems (DIS)*. ACM, New York, NY, USA, 975–984. https://doi.org/10.1145/2598510.2598579
[58] Hana Habib and Lorrie Faith Cranor. 2022. Evaluating the usability of privacy choice mechanisms. In *Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, Berkeley, CA, USA, 273–289. https://www.usenix.org/system/files/soups2022-habib.pdf.
[59] Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2020. "It's a scavenger hunt": Usability of Websites' Opt-Out and Data Deletion Choices. In *ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 384:1–384:12. https://doi.org/10.1145/3313831.3376511
[60] André Hajek and Hans-Helmut König. 2021. Social isolation and loneliness of older adults in times of the COVID-19 pandemic: Can use of online social media sites and video chats assist in mitigating social isolation and loneliness? *Gerontology* 67, 1 (2021), 121–123. https://doi.org/10.1159/000512793
[61] Riitta Hänninen, Sakari Taipale, and Raija Luostari. 2021. Exploring heterogeneous ICT use among older adults: The warm experts' perspective. *New Media & Society* 23, 6 (2021), 1584–1601. https://doi.org/10.1177/1461444820917353
[62] Franziska Herbert, Steffen Becker, Annalina Buckmann, Marvin Kowalewski, Jonas Hielscher, Yasemin Acar, Markus Dürmuth, Yixin Zou, and M. Angela Sasse. 2024. Digital Security — A Question of Perspective. A Large-Scale Telephone Survey with Four At-Risk User Groups. In *IEEE Symposium on Security and Privacy*. IEEE, New York, NY, USA, 1–20.
[63] Paul Hitlin and Lee Rainie. 2019. *Facebook algorithms and personal data.* Technical Report. Pew Research Center. https://www.pewresearch.org/internet/2019/01/16/facebook-algorithms-and-personal-data/. Accessed: 2023-02-28.
[64] Rae Hodge. 2022. Zoom privacy risks: The video chat app could be sharing more information than you think. https://www.cnet.com/tech/services-and-software/zoom-privacy-risks-the-video-chat-app-could-be-sharing-more-information-than-you-think/. Accessed: 2023-02-28.
[65] Tamara E Holmes. 2021. Elder Financial Abuse: Stopping Fraud in the Family. https://www.aarp.org/money/scams-fraud/info-2021/family-elder-fraud.html. Accessed: 2023-02-28.
[66] Chris Jay Hoofnagle, Jennifer King, Su Li, and Joseph Turow. 2010. How different are young adults from older adults when it comes to information privacy attitudes and policies? https://doi.org/10.2139/ssrn.1589864. Accessed: 2023-02-28.
[67] Lesa Lorenzen Huber, Kalpana Shankar, Kelly Caine, Kay Connelly, L Jean Camp, Beth Ann Walker, and Lisa Borrero. 2013. How in-home technologies mediate caregiving relationships in later life. *International Journal of Human-Computer Interaction* 29, 7 (2013), 441–455. https://doi.org/10.1080/10447318.2012.715990
[68] Judith E Hupcey, Mary Beth Clark, Cristina R Hutcheson, and Virginia L Thompson. 2004. Expectations for care: Older adults' satisfaction with and trust in health care providers. *Journal of Gerontological Nursing* 30, 11 (2004), 37–45. https://doi.org/10.3928/0098-9134-20041101-11
[69] Jane Im, Jill Dimond, Melody Berton, Una Lee, Katherine Mustelier, Mark S Ackerman, and Eric Gilbert. 2021. Yes: Affirmative consent as a theoretical framework for understanding and imagining social platforms. In *ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 403:1–403:18. https://doi.org/10.1145/3411764.3445778
[70] Efraim Jaul and Jeremy Barron. 2017. Age-related diseases and clinical and public health implications for the 85 years old and over population. *Frontiers in public health* 5 (2017), 335:1–335:7. https://doi.org/10.3389/fpubh.2017.00335
[71] Hyun Gu Kang, Diane F Mahoney, Helen Hoenig, Victor A Hirth, Paolo Bonato, Ihab Hajjar, and Lewis A Lipsitz. 2010. In situ monitoring of health in older adults: technologies and issues. *Journal of the American Geriatrics Society* 58, 8 (2010), 1579–1586. https://doi.org/10.1111/j.1532-5415.2010.02959.x
[72] Sanja Kapidzic and Susan C Herring. 2015. Race, gender, and self-presentation in teen profile photographs. *New Media & Society* 17, 6 (2015), 958–976. https://doi.org/10.1177/1461444813520301
[73] Murat Kezer, Barış Sevi, Zeynep Cemalcilar, and Lemi Baruh. 2016. Age differences in privacy attitudes, literacy and privacy management on Facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 10, 1 (2016), 2:1–2:20. https://doi.org/10.5817/CP2016-1-2
[74] Bran Knowles, Vicki L Hanson, Yvonne Rogers, Anne Marie Piper, Jenny Waycott, Nigel Davies, Aloha Hufana Ambe, Robin N Brewer, Debaleena Chattopadhyay, Marianne Dee, et al. 2021. The harm in conflating aging with accessibility.

Commun. ACM 64, 7 (2021), 66–71. https://doi.org/10.1145/3431280
[75] Jess Kropczynski, Zaina Aljallad, Nathan Jeffrey Elrod, Heather Lipford, and Pamela J Wisniewski. 2021. Towards building community collective efficacy for managing digital privacy and security within older adult communities. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW3 (2021), 255:1–255:27. https://doi.org/10.1145/3432954
[76] Celine Latulipe, Amy Gatto, Ha T Nguyen, David P Miller, Sara A Quandt, Alain G Bertoni, Alden Smith, and Thomas A Arcury. 2015. Design considerations for patient portal adoption by low-income, older adults. In *ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 3859–3868. https://doi.org/10.1145/2702123.2702392
[77] Pedro Giovanni Leon, Justin Cranshaw, Lorrie Faith Cranor, Jim Graves, Manoj Hastak, Blase Ur, and Guzi Xu. 2012. What do online behavioral advertising privacy disclosures communicate to users?. In *Workshop on Privacy in the Electronic Society (WPES)*. ACM, New York, NY, USA, 19–30. https://doi.org/10.1145/2381966.2381970
[78] Calvin A Liang, Sean A Munson, and Julie A Kientz. 2021. Embracing four tensions in human-computer interaction research with marginalized people. *ACM Transactions on Computer-Human Interaction (TOCHI)* 28, 2 (2021), 14:1–14:47. https://doi.org/10.1145/3443686
[79] Chen Ling, Utkucan Balcı, Jeremy Blackburn, and Gianluca Stringhini. 2021. A first look at zoombombing. In *IEEE Symposium on Security and Privacy*. IEEE, New York, NY, USA, 1452–1467. https://doi.org/10.1109/SP40001.2021.00061
[80] Simi Linton. 2017. Reassigning meaning. In *Beginning with Disability*. Routledge, Milton Park, United Kingdom, 20–27. https://doi.org/10.4324/9781315453217-3
[81] Eden Litt and Eszter Hargittai. 2014. A bumpy ride on the information superhighway: Exploring turbulence online. *Computers in Human Behavior* 36 (2014), 520–529. https://doi.org/10.1016/j.chb.2014.04.027
[82] Lili Liu, Eleni Stroulia, Ioanis Nikolaidis, Antonio Miguel-Cruz, and Adriana Rios Rincon. 2016. Smart homes and home health monitoring technologies for older adults: A systematic review. *International journal of medical informatics* 91 (2016), 44–59. https://doi.org/10.1016/j.ijmedinf.2016.04.007
[83] Lesa Lorenzen-Huber, Mary Boutain, L Jean Camp, Kalpana Shankar, and Kay H Connelly. 2011. Privacy, technology, and aging: A proposed framework. *Ageing International* 36, 2 (2011), 232–252. https://doi.org/10.1007/s12126-010-9083-y
[84] Marika Lüders and Petter Bae Brandtzæg. 2017. 'My children tell me it's so simple': A mixed-methods approach to understand older non-users' perceptions of Social Networking Sites. *New Media & Society* 19, 2 (2017), 181–198. https://doi.org/10.1177/1461444814554064
[85] João Mariano, Sibila Marques, Miguel R Ramos, Filomena Gerardo, Cátia Lage da Cunha, Andrey Girenko, Jan Alexandersson, Bernard Stree, Michele Lamanna, Maurizio Lorenzatto, et al. 2022. Too old for technology? Stereotype threat and technology use by older adults. *Behaviour & Information Technology* 41, 7 (2022), 1503–1514. https://doi.org/10.1080/0144929X.2021.1882577
[86] MarketingCharts.com. 2019. Older Adults Show Greater Propensity to Click on Social Video Ads. https://www.marketingcharts.com/advertising-trends/creative-and-formats-109928. Accessed: 2023-02-28.
[87] Peter Mayer, Collins W Munyendo, Michelle L Mazurek, and Adam J Aviv. 2022. Why Users (Don't) Use Password Managers at a Large Educational Institution. In *USENIX Security Symposium*. USENIX Association, Berkeley, CA, USA, 1849–1866. https://www.usenix.org/system/files/sec22-mayer.pdf.
[88] Allison McDonald, Carlo Sugatan, Tamy Guberek, and Florian Schaub. 2021. The Annoying, the Disturbing, and the Weird: Challenges with Phone Numbers as Identifiers and Phone Number Recycling. In *ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 559:1–559:14. https://doi.org/10.1145/3411764.3445085
[89] Nora McDonald and Andrea Forte. 2020. The politics of privacy theories: Moving from norms to vulnerabilities. In *ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 40:1–40:14. https://doi.org/10.1145/3313831.3376167
[90] Nora McDonald and Helena M Mentis. 2021. Building for 'we': safety settings for couples with memory concerns. In *ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 554:1–554:11. https://doi.org/10.1145/3411764.3445071
[91] Nora Mcdonald and Helena M Mentis. 2021. "Citizens Too": safety setting collaboration among older adults with memory concerns. *ACM Transactions on Computer-Human Interaction (TOCHI)* 28, 5 (2021), 31:1–31:32. https://doi.org/10.1145/3465217
[92] William Melicher, Mahmood Sharif, Joshua Tan, Lujo Bauer, Mihai Christodorescu, and Pedro Giovanni Leon. 2016. Preferences for web tracking. *Proceedings on Privacy Enhancing Technologies* 2 (2016), 135–154. https://doi.org/10.1515/popets-2016-0009
[93] Helena M Mentis, Galina Madjaroff, Aaron Massey, and Zoya Trendafilova. 2020. The Illusion of Choice in Discussing Cybersecurity Safeguards Between Older Adults with Mild Cognitive Impairment and Their Caregivers. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2 (2020), 164:1–164:19. https://doi.org/10.1145/3415235
[94] Helena M Mentis, Galina Madjaroff, and Aaron K Massey. 2019. Upside and downside risk in online security for older adults with mild cognitive impairment. In *ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 343:1–343:13. https://doi.org/10.1145/3290605.3300573
[95] Meta. 2023. How do I choose to see less of certain ad topics while on Facebook? https://www.facebook.com/help/353660662271696. Accessed: 2023-02-28.
[96] Brooke Migdon. 2021. Why experts say you don't need antivirus software anymore. https://thehill.com/changing-america/enrichment/arts-culture/583831-why-experts-say-you-dont-need-antivirus-software/. Accessed: 2023-02-28.
[97] Albert Munanga. 2019. Cybercrime: A new and growing problem for older adults. *Journal of gerontological nursing* 45, 2 (2019), 3–5. https://doi.org/10.3928/00989134-20190111-01
[98] Savanthi Murthy, Karthik S Bhat, Sauvik Das, and Neha Kumar. 2021. Individually vulnerable, collectively safe: The security and privacy practices of households with older adults. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (2021), 138:1–138:24. https://doi.org/10.1145/3449212
[99] Elizabeth D Mynatt, A-S Melenhorst, A-D Fisk, and Wendy A Rogers. 2004. Aware technologies for aging in place: understanding user needs and attitudes. *IEEE Pervasive Computing* 3, 2 (2004), 36–41. https://doi.org/10.1109/MPRV.2004.1316816
[100] Tobias Nef, Raluca L Ganea, René M Müri, and Urs P Mosimann. 2013. Social networking sites and older users-a systematic review. *International psychogeriatrics* 25, 7 (2013), 1041–1053. https://doi.org/10.1017/S1041610213000355
[101] James Nicholson, Lynne Coventry, and Pamela Briggs. 2019. "If It's Important It Will Be A Headline" Cybersecurity Information Seeking in Older Adults. In *ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 349:1–349:11. https://doi.org/10.1145/3290605.3300579
[102] James Nicholson, Ben Morrison, Matt Dixon, Jack Holt, Lynne Coventry, and Jill McGlasson. 2021. Training and Embedding Cybersecurity Guardians in Older Communities. In *ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 86:1–86:15. https://doi.org/10.1145/3411764.3445078
[103] Helen Nissenbaum. 2009. *Privacy in context*. Stanford University Press, Stanford, CA, USA.
[104] Daniela Oliveira, Harold Rocha, Huizi Yang, Donovan Ellis, Sandeep Dommaraju, Melis Muradoglu, Devon Weir, Adam Soliman, Tian Lin, and Natalie Ebner. 2017. Dissecting spear phishing emails for older vs young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing. In *ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 6412–6424. https://doi.org/10.1145/3025453.3025831
[105] Cheul Young Park, Cori Faklaris, Siyan Zhao, Alex Sciuto, Laura Dabbish, and Jason Hong. 2018. Share and share alike? An exploration of secure behaviors in romantic relationships. In *Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, Berkeley, CA, USA, 83–102. https://www.usenix.org/system/files/conference/soups2018/soups2018-park.pdf.
[106] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2019. Why people (don't) use password managers effectively. In *Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, Berkeley, CA, USA, 319–338. https://www.usenix.org/system/files/soups2019-pearman.pdf.
[107] Rebecca Pifer. 2023. Healthcare industry most common victim of third-party breaches, Black Kite finds. https://www.healthcaredive.com/news/healthcare-cybersecurity-third-party-breaches-killnet-hhs/641840/. Accessed: 2023-02-28.
[108] Barbara Plagg, Adolf Engl, Giuliano Piccoliori, and Klaus Eisendle. 2020. Prolonged social isolation of the elderly during COVID-19: Between benefit and damage. *Archives of Gerontology and Geriatrics* 89 (2020), 104086. https://doi.org/10.1016/j.archger.2020.104086
[109] Shannon Power. 2023. Apple Goes Viral for Appearing to Host iPhone Class for Older Customers. https://www.newsweek.com/apple-iphone-classes-twitter-smartphone-elderly-older-customers-1772345. Accessed: 2023-02-28.
[110] Andrea Prati, Caifeng Shan, and Kevin I-Kai Wang. 2019. Sensors, vision and networks: From video surveillance to activity recognition and health monitoring. *Journal of Ambient Intelligence and Smart Environments* 11, 1 (2019), 5–22. https://doi.org/10.3233/AIS-180510
[111] Anabel Quan-Haase and Isioma Elueze. 2018. Revisiting the privacy paradox: Concerns and protection strategies in the social media experiences of older adults. In *International Conference on Social Media and Society*. ACM, New York, NY, USA, 150–159. https://doi.org/10.1145/3217804.3217907
[112] Anabel Quan-Haase and Dennis Ho. 2020. Online privacy concerns and privacy protection strategies among older adults in East York, Canada. *Journal of the Association for Information Science and Technology* 71, 9 (2020), 1089–1102. https://doi.org/10.1002/asi.24364
[113] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J Aviv. 2021. "Warn Them" or "Just Block Them"?: Investigating Privacy Concerns Among Older and Working Age Adults. *Proceedings on Privacy Enhancing Technologies* 2021, 2 (2021), 21–47. https://doi.org/10.2478/popets-2021-0016

[114] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J Aviv. 2021. Why Older Adults (Don't) Use Password Managers. In *USENIX Security Symposium*. USENIX Association, Berkeley, CA, USA, 73–90. https://www.usenix.org/system/files/sec21-ray.pdf.

[115] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. 2016. How I learned to be secure: a census-representative survey of security advice sources and behavior. In *ACM Conference on Computer and Communications Security (CCS)*. ACM, New York, NY, USA, 666–677. https://doi.org/10.1145/2976749.2978307

[116] Robert W Reeder, Iulia Ion, and Sunny Consolvo. 2017. 152 simple steps to stay safe online: Security advice for non-tech-savvy users. *IEEE Security & Privacy* 15, 5 (2017), 55–64. https://doi.org/10.1109/MSP.2017.3681050

[117] Kat Roemmich, Florian Schaub, and Nazanin Andalibi. 2023. Emotion AI at Work: Implications for Workplace Surveillance, Emotional Labor, and Emotional Privacy. In *ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 558:1–558:20. https://doi.org/10.1145/3544548.3580950

[118] Michael Ross, Igor Grossmann, and Emily Schryer. 2014. Contrary to psychological and popular opinion, there is no compelling evidence that older adults are disproportionately victimized by consumer fraud. *Perspectives on Psychological Science* 9, 4 (2014), 427–442. https://doi.org/10.1177/1745691614535935

[119] Dawn K Sakaguchi-Tang, Alyssa L Bosold, Yong K Choi, and Anne M Turner. 2017. Patient portal use and experience among older adults: systematic review. *JMIR medical informatics* 5, 4 (2017), e38. https://doi.org/10.2196/medinform.8092

[120] Marc Saltzman. 2022. Elder fraud is real. Tell your parents, grandparents, and friends about these scams. https://eu.usatoday.com/story/tech/2022/09/18/cybercrime-cost-american-seniors-3-billion-last-year-62-jump/10420029002/. Accessed: 2023-02-28.

[121] Shruti Sannon and Andrea Forte. 2022. Privacy Research with Marginalized Groups: What We Know, What's Needed, and What's Next. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (2022), 455:1–455:33. https://doi.org/10.1145/3555556

[122] Tali Sharot. 2011. The optimism bias. *Current biology* 21, 23 (2011), R941–R945.

[123] Hu Shuijing and Jiang Tao. 2017. An empirical study on digital privacy risk of senior citizens. In *International Conference on Robots & Intelligent System*. IEEE, New York, NY, USA, 19–24. https://doi.org/10.1109/ICRIS.2017.13

[124] Lucy Simko. 2022. *Humans and Vulnerability During Times of Change: Computer Security Needs, Practices, Challenges, and Opportunities*. Ph.D. Dissertation. University of Washington.

[125] Joseph Simons, Noah Joshua Phillips, Rohit Chopra, Rebecca Kelly Slaughter, and Christine S. Wilson. 2020. *Protecting Older Consumers*. Technical Report. The Federal Trade Commission. https://www.ftc.gov/system/files/documents/reports/protecting-older-consumers-2019-2020-report-federal-trade-commission/p144400_protecting_older_adults_report_2020.pdf.

[126] Supriya Singh, Anuja Cabraal, Catherine Demosthenous, Gunela Astbrink, and Michele Furlong. 2007. Password sharing: implications for security design based on social practice. In *ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 895–904. https://doi.org/10.1145/1240624.1240759

[127] Julia Slupska, Selina Cho, Marissa Begonia, Ruba Abu-Salma, Nayanatara Prakash, and Mallika Balakrishnan. 2022. "They Look at Vulnerability and Use That to Abuse You": Participatory Threat Modelling with Migrant Domestic Workers. In *USENIX Security Symposium*. USENIX Association, Berkeley, CA, USA, 323–340. https://www.usenix.org/system/files/sec22-slupska-vulnerability.pdf.

[128] Daniel J Solove. 2006. A taxonomy of privacy. *University of Pennsylvania law review* 154, 3 (2006), 477–564. https://doi.org/10.2307/40041279

[129] Daniel J Solove. 2007. I've got nothing to hide and other misunderstandings of privacy. *San Diego Law Review* 44 (2007), 745–772. https://heinonline.org/HOL/Page?handle=hein.journals/sanlr44&div=40&collection=journals.

[130] Daniel J Solove. 2012. Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review* 126 (2012), 1880–1903. https://heinonline.org/HOL/Page?handle=hein.journals/hlr126&div=87&collection=journals.

[131] Daniel J Solove. 2021. The myth of the privacy paradox. *George Washington Law Review* 89 (2021), 1–51. https://heinonline.org/HOL/Page?handle=hein.journals/gwlr89&div=4.

[132] Peter Story, Daniel Smullen, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2020. From intent to action: Nudging users towards secure mobile payments. In *Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, Berkeley, CA, USA, 379–415. https://www.usenix.org/system/files/soups2020-story.pdf.

[133] Sakari Taipale, Tomi Oinas, and Joonas Karhinen. 2021. Heterogeneity of traditional and digital media use among older adults: A six-country comparison. *Technology in Society* 66 (2021), 101642. https://doi.org/10.1016/j.techsoc.2021.101642

[134] Xinru Tang, Yuling Sun, Bowen Zhang, Zimi Liu, RAY LC, Zhicong Lu, and Xin Tong. 2022. "I Never Imagined Grandma Could Do So Well with Technology" Evolving Roles of Younger Family Members in Older Adults' Technology Learning and Use. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (2022), 478:1–478:29. https://doi.org/10.1145/3555579

[135] Jiang Tao and Hu Shuijing. 2016. The elderly and the big data: how older adults deal with digital privacy. In *IEEE International Conference on Intelligent Transportation, Big Data & Smart City*. IEEE, New York, NY, USA, 285–288. https://doi.org/10.1109/ICITBS.2016.35

[136] Janelle S Taylor, Shaune M DeMers, Elizabeth K Vig, and Soo Borson. 2012. The disappearing subject: exclusion of people with cognitive impairment and dementia from geriatrics research. *Journal of the American Geriatrics Society* 60, 3 (2012), 413–419. https://doi.org/10.1111/j.1532-5415.2011.03847.x

[137] Stephanie Tonneson. 2022. Zoom Becomes Video Conferencing Leader During COVID-19. Why? https://pipeline.zoominfo.com/marketing/zoom-video-growth-coronavirus. Accessed: 2023-02-28.

[138] Daphne Townsend, Frank Knoefel, and Rafik Goubran. 2011. Privacy versus autonomy: a tradeoff model for smart home monitoring technologies. In *International Conference of the IEEE Engineering in Medicine and Biology Society*. IEEE, New York, NY, USA, 4749–4752. https://doi.org/10.1109/IEMBS.2011.6091176

[139] Sabine Trepte, Doris Teutsch, Philipp K Masur, Carolin Eicher, Mona Fischer, Alisa Hennhöfer, and Fabienne Lind. 2015. Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In *Reforming European data protection law*. Springer, New York, NY, USA, 333–365. https://doi.org/10.1007/978-94-017-9385-8_14

[140] Daniel W Turner III. 2010. Qualitative interview design: A practical guide for novice investigators. *The Qualitative Report* 15, 3 (2010), 754–760. http://www.nova.edu/ssss/QR/QR15-3/qid.pdf.

[141] United States Census Bureau. 2021. Computer and Internet Use in the United States: 2018. https://www.census.gov/newsroom/press-releases/2021/computer-internet-use.html. Accessed: 2023-02-28.

[142] United States Census Bureau. 2021. Educational Attainment in the United States: 2020. https://www.census.gov/data/tables/2020/demo/educational-attainment/cps-detailed-tables.html. Accessed: 2023-02-28.

[143] United States Census Bureau. 2021. National Demographic Analysis Tables: 2020. https://www.census.gov/data/tables/2020/demo/popest/2020-demographic-analysis-tables.html. Accessed: 2023-02-28.

[144] Blase Ur, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. 2012. Smart, useful, scary, creepy: perceptions of online behavioral advertising. In *Symposium on Usable Privacy and Security (SOUPS)*. ACM, New York, NY, USA, 4:1–4:15. https://doi.org/10.1145/2335356.2335362

[145] U.S. Department of Health & Human Services. 2021. *Indicator Definitions – Older Adults*. Centers for Disease Control and Prevention. https://www.cdc.gov/cdi/definitions/older-adults.html. Accessed: 2023-02-28.

[146] Evert Van den Broeck, Karolien Poels, and Michel Walrave. 2015. Older and wiser? Facebook use, privacy concern, and privacy protection in the life stages of emerging, young, and middle adulthood. *Social Media + Society* 1, 2 (2015), 1–11. https://doi.org/10.1177/2056305115616149

[147] Aafke Victoor, Diana MJ Delnoij, Roland D Friele, and Jany JDJM Rademakers. 2012. Determinants of patient choice of healthcare providers: a scoping review. *BMC health services research* 12 (2012), 272:1–272:16. https://doi.org/10.1186/1472-6963-12-272

[148] John Vines, Roisin McNaney, Rachel Clarke, Stephen Lindsay, John McCarthy, Steve Howard, Mario Romero, and Jayne Wallace. 2013. Designing for-and with-vulnerable people. In *ACM Conference on Human Factors in Computing Systems (CHI): Extended Abstracts*. ACM, New York, NY, USA, 3231–3234. https://doi.org/10.1145/2468356.2479654

[149] Jessica Vitak, Yuting Liao, Mega Subramaniam, and Priya Kumar. 2018. "I Knew It Was Too Good to Be True:" The Challenges Economically Disadvantaged Internet Users Face in Assessing Trustworthiness, Avoiding Scams, and Developing Self-Efficacy Online. *Proceedings of the ACM on human-computer interaction* 2, CSCW (2018), 176:1–176:25. https://doi.org/10.1145/3274445

[150] Helena Blažun Vošner, Samo Bobek, Peter Kokol, and Marija Javornik Krečič. 2016. Attitudes of active older Internet users towards online social networking. *Computers in Human Behavior* 55 (2016), 230–241. https://doi.org/10.1016/j.chb.2015.09.014

[151] Ashley Marie Walker, Yaxing Yao, Christine Geeng, Roberto Hoyle, and Pamela Wisniewski. 2019. Moving beyond'one size fits all' research considerations for working with vulnerable populations. *Interactions* 26, 6 (2019), 34–39. https://doi.org/10.1145/3358904

[152] Serena Wang, Cori Faklaris, Junchao Lin, Laura Dabbish, and Jason I Hong. 2022. 'It's Problematic but I'm not Concerned': University Perspectives on Account Sharing. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW1 (2022), 68:1–68:27. https://doi.org/10.1145/3512915

[153] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L Mazurek, Manya Sleeper, and Kurt Thomas. 2022. Sok: A framework for unifying at-risk user research. In *IEEE Symposium on Security and Privacy*. IEEE, New York, NY, USA, 2344–2360. https://doi.org/10.1109/SP46214.2022.9833643

[154] Hue Watson, Eyitemi Moju-Igbene, Akanksha Kumari, and Sauvik Das. 2020. "We Hold Each Other Accountable": Unpacking How Social Groups Approach Cybersecurity and Privacy Together. In *ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 478:1–478:12. https:

//doi.org/10.1145/3313831.3376605
[155] Jenny Waycott, Greg Wadley, Stefan Schutt, Arthur Stabolidis, and Reeva Lederman. 2015. The Challenge of Technology Research in Sensitive Settings: Case Studies in 'Sensitive HCI'. In *OzCHI '15: Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer-Human Interaction*. ACM, New York, NY, USA, 240–249. https://doi.org/10.1145/2838739.2838773
[156] Miranda Wei, Madison Stamos, Sophie Veys, Nathan Reitinger, Justin Goodman, Margot Herman, Dorota Filipczuk, Ben Weinshel, Michelle L Mazurek, and Blase Ur. 2020. What Twitter knows: characterizing ad targeting practices, user perceptions, and ad explanations through users' own Twitter data. In *USENIX Security Symposium*. USENIX Association, Berkeley, CA, USA, 145–162. https://www.usenix.org/system/files/sec20-wei.pdf.
[157] Monica Whitty, James Doodson, Sadie Creese, and Duncan Hodges. 2015. Individual differences in cyber security behaviors: an examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking* 18, 1 (2015), 3–7. https://doi.org/10.1089/cyber.2014.0179
[158] Katherine Wild, Linda Boise, Jay Lundell, and Anna Foucek. 2008. Unobtrusive in-home monitoring of cognitive and physical health: Reactions and perceptions of older adults. *Journal of Applied Gerontology* 27, 2 (2008), 181–200. https://doi.org/10.1177/0733464807311435
[159] World Health Organization. 2018. Ageing and health. https://www.who.int/news-room/fact-sheets/detail/ageing-and-health. Accessed: 2023-02-28.
[160] Heng Xu and Nan Zhang. 2022. From contextualizing to context theorizing: assessing context effects in privacy research. *Management Science* 68, 10 (2022), 7383–7401. https://doi.org/10.1287/mnsc.2021.4249
[161] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019. Defending my castle: A co-design study of privacy mechanisms for smart homes. In *ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 198:1–198:12. https://doi.org/10.1145/3290605.3300428
[162] Yaxing Yao, Davide Lo Re, and Yang Wang. 2017. Folk models of online behavioral advertising. In *ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW)*. ACM, New York, NY, USA, 1957–1969. https://doi.org/10.1145/2998181.2998316
[163] Chiara Zanchetta, Hannah Schiff, Carolina Novo, Sandra Cruz, and Carlos Vaz de Carvalho. 2022. Generational Inclusion: Getting Older Adults Ready to Own Safe Online Identities. *Education Sciences* 12, 10 (2022), 715. https://doi.org/10.3390/educsci12100715
[164] Eva-Maria Zeissig, Chantal Lidynia, Luisa Vervier, Andera Gadeib, and Martina Ziefle. 2017. Online privacy perceptions of older adults. In *International Conference on Human Aspects of IT for the Aged Population*. Springer, New York, NY, USA, 181–200. https://doi.org/10.1007/978-3-319-58536-9_16
[165] Eric Zeng, Tadayoshi Kohno, and Franziska Roesner. 2021. What makes a "bad" ad? user perceptions of problematic online advertising. In *ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 361:1–361:24. https://doi.org/10.1145/3411764.3445459
[166] Eric Zeng, Rachel McAmis, Tadayoshi Kohno, and Franziska Roesner. 2022. What factors affect targeting and bids in online advertising? a field measurement study. In *ACM Internet Measurement Conference (IMC)*. ACM, New York, NY, USA, 210–229. https://doi.org/10.1145/3517745.3561460
[167] Jiaxi Zhang, Jiaxi Peng, Pan Gao, He Huang, Yunfei Cao, Lulu Zheng, and Danmin Miao. 2019. Relationship between meaning in life and death anxiety in the elderly: self-esteem as a mediator. *BMC geriatrics* 19 (2019), 308:1–308:8. https://doi.org/10.1186/s12877-019-1316-7
[168] Matthias Ziegler, Erik Danay, Moritz Heene, Jens Asendorpf, and Markus Bühner. 2012. Openness, fluid intelligence, and crystallized intelligence: Toward an integrative model. *Journal of Research in Personality* 46, 2 (2012), 173–183.
[169] Yixin Zou, Abraham H Mhaidli, Austin McCall, and Florian Schaub. 2018. "I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach. In *Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, Berkeley, CA, USA, 197–216. https://www.usenix.org/system/files/conference/soups2018/soups2018-zou.pdf.
[170] Yixin Zou, Kevin Roundy, Acar Tamersoy, Saurabh Shintre, Johann Roturier, and Florian Schaub. 2020. Examining the adoption and abandonment of security, privacy, and identity theft protection practices. In *ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 443:1–443:15. https://doi.org/10.1145/3313831.3376570
[171] Shoshana Zuboff. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile Books, London, United Kingdom.

A PARTICIPANT DETAILS

Individual Characteristics	N	%
Annual Household Income[4]		
Less than $25k	6	14.0%
$25 - $50k	13	30.2%
$50 - $75k	9	20.9%
$75 - $100k	8	18.6%
$100 - $150k	3	7.0%
More than $150k	3	7.0%
Education Attainment		
High school	1	2.3%
Some college	6	14.0%
Associate's degree	4	9.3%
Bachelor's degree	17	39.5%
Master's degree	12	27.9%
Doctorate	3	7.0%
Race/Ethnicity[5]		
American Indian	2	4.7%
Asian	2	4.7%
Black/African American	12	27.9%
Hispanic	3	7.0%
White	26	60.5%
Other (Middle Eastern, multi-race)	2	4.7%
Self-Reported Health Condition		
Excellent	4	9.3%
Good	23	53.5%
Fair	13	30.2%
Poor	3	7.0%
Housing		
Own or rented home	39	90.7%
Senior residential community	3	7.0%
Nursing home	1	2.3%
Caregiver		
No one	35	81.4%
Informal caregiver	7	16.3%
Hired/Professional caregiver	1	2.3%

Table 1: Participant characteristics (n=43).

[4]There was one non-response for income.
[5]The percentage adds up to more than 100% since one can select multiple options.