Privacy and Security Threat Models and Mitigation Strategies of Older Adults

Alisa Frik,[1,2] Leysan Nurgalieva,[3] Julia Bernd,[1] Joyce S. Lee,[2] Florian Schaub,[4] Serge Egelman[1,2]
[1]*International Computer Science Institute (ICSI)*
[2]*University of California, Berkeley*
[3]*University of Trento*
[4]*University of Michigan*
afrik@icsi.berkeley.edu, leysan.nurgalieva@unitn.it, jbernd@icsi.berkeley.edu,
joyce@ischool.berkeley.edu, fschaub@umich.edu, egelman@cs.berkeley.edu

Abstract

Older adults (65+) are becoming primary users of emerging smart systems, especially in health care. However, these technologies are often not designed for older users and can pose serious privacy and security concerns due to their novelty, complexity, and propensity to collect and communicate vast amounts of sensitive information. Efforts to address such concerns must build on an in-depth understanding of older adults' perceptions and preferences about data privacy and security for these technologies, and accounting for variance in physical and cognitive abilities. In semi-structured interviews with 46 older adults, we identified a range of complex privacy and security attitudes and needs specific to this population, along with common threat models, misconceptions, and mitigation strategies. Our work adds depth to current models of how older adults' limited technical knowledge, experience, and age-related declines in ability amplify vulnerability to certain risks; we found that health, living situation, and finances play a notable role as well. We also found that older adults often experience usability issues or technical uncertainties in mitigating those risks—and that managing privacy and security concerns frequently consists of limiting or avoiding technology use. We recommend educational approaches and usable technical protections that build on seniors' preferences.

1 Introduction

Due to increasing life expectancy, the number of people in the U.S. over 65 is expected to double by 2060 [79]. The need for professional care is rising accordingly, while the labor market for caregivers is projected to shrink [59]. These factors are stimulating investment in emerging "smart" technologies for older adults—aimed at sustaining independent living, increasing quality of life, and mitigating health issues via early detection [83]. Emerging smart technologies such as wearable medical devices, fall sensors, and therapeutic robots [10] may yield benefits, but due to their novelty, complexity, and propensity to collect vast amounts of information, they also pose security and privacy risks.

Due to limited technological literacy and experience, and because of declining physical and mental abilities [44, 96], older adults are particularly unaware of and susceptible to those privacy and security risks [5, 16]. Specifically, older adults have less knowledge of Internet security hazards [36, 40], use technology less frequently [19, 28, 40, 43, 52, 101], are more vulnerable to security risks [41], and are more often targeted for attacks [48] than younger populations. Lack of security knowledge and experience generally correlates with riskier behaviors [45, 71, 73]. Indeed, older adults seem generally less likely to protect against privacy and security risks [57, 62, 85, 99, 101]—though the subject of older adults' privacy management has not been investigated comprehensively.

While seniors often express privacy and (to a lesser extent) security concerns in relation to technology [35, 64, 87], their views are underrepresented in privacy and security research. At the same time, the limited literature on the topic shows that privacy preferences of older adults are heterogeneous [36] and fine-grained [16, 47], and thus warrant further exploration.

The goal of our research is to inform the design of effective systems that empower older adults to make informed decisions, to have better control over their personal data, and to maintain better security practices. To this end, we conducted semi-structured interviews with 46 older adults (65–95 years old). We identify their common security and privacy concerns and threat models, behaviors and strategies to mitigate perceived risks, usability issues with current protections, learning and troubleshooting approaches, and misconceptions regarding security and privacy.

We add depth to current models of how older adults'

USENIX Symposium on Usable Privacy and Security (SOUPS) 2019.
August 11–13, 2019, Santa Clara, CA, USA.

relatively low technical knowledge and experience and age-related declines in abilities amplify their vulnerability to certain risks, and found that health and living situations and financial considerations also play an important role. We also found that older adults often experience usability issues or technical uncertainties in mitigating those risks—and that managing privacy and security concerns frequently entails them limiting or simply avoiding use of new technologies. Based on the identified preferences of older adults, we offer privacy- and security-enhancing recommendations for product developers and for educational efforts.

2 Related Work

Technological solutions aiming to meet older adults' needs span different domains (e.g., health, nutrition, safety, or navigation [10]) and forms (e.g., wearable, ambient, or camera-based devices [98]). Both aspects factor into what data is collected: wearable devices, for instance, enable collection of orientation, movement, and vital signs with embedded gyroscopes, accelerometers, and other sensors [56, 92]. Context-aware systems use sensors as well, often with the addition of image capture, computer vision, and artificial intelligence to monitor activities or to detect anomalies [e.g., 20, 31]. Likewise, dynamic care robots [e.g., 3, 51, 74] leverage sensors and sometimes cameras for medication management or companionship. Many emerging technologies are connected via Wi-Fi, Zigbee, or similar protocols [e.g., 77, 86], integrating wearable devices with context-aware sensors into a larger ecosystem.

The effectiveness and quality of assistance in critical situations often rely on collecting extensive data. However, extensive monitoring and surveillance trigger privacy and security concerns among users of such technologies [35, 64, 87].

Older adults' privacy concerns and risk perceptions are often different from the concerns of the better-studied younger population [34, 36]. Trust has been identified as a core factor affecting older adults' adoption of ubiquitous computing technologies [22, 24, 65]. However, Knowles and Hanson [54] found that the language of (dis)trust was more relevant to larger value-related issues around digital technologies than to practical decision-making about adoption.

Knowles and Hanson therefore argue that technology adoption should not be viewed as indicating trust or acceptability [54]. Seniors' concerns about monitoring systems include invisible audiences, and absence of feedback when systems are in use or when data is accessed [92]. Other research suggests that some seniors are concerned about who accesses data, how often, and at what level of detail [4, 47, 49]. Although older adults tend to rely on family members in "dealing with technology" [47, 75], delegation of security choices should not be considered a safe behavioral strategy [32].Additionally, older adults may have misperceptions about security, for example, due to over-reliance on surface cues and affordances[e.g., 47].

On the other hand, misconceptions about data collection may raise false concerns that can be mitigated by appropriate explanations [97]. Older adults are also capable of using data controls and security strategies in certain cases, such as basic password encryption [14, 47]. Furthermore, individual differences are found to heavily affect privacy and security preferences: seniors with severe health conditions are more likely to share their information [11, 97] and generally value independence and safety more than privacy [26, 27, 67].

Seniors also represent a more heterogeneous population than younger people [39, 60], due to differences in their health conditions, education, living conditions, and experience. Physical and cognitive impairments may further complicate usability issues. These findings suggest that older adults' privacy and security attitudes and mental models are context-dependent and heterogeneous in nature.

3 Methods

We conducted 1–1.5 hour semi-structured in-person interviews, in which we discussed: (1) privacy- and security-related concerns and threats and (2) risk management strategies.[1]

We reached out to inhabitants of nursing homes and senior residences, members of senior centers, and organizations for retired people in the San Francisco Bay Area. We screened potential participants using surveys in several formats—online, phone, paper, and in person—but excluded individuals with serious cognitive impairments and non-English speakers. With IRB approval, we conducted interviews in May–June 2018 with 46 participants at their residences or at public senior centers (their choice). We paid $20 as compensation. We administered exit surveys about participants' individual characteristics.

The structure of our interviews was inspired by Zeng et al. [100], who interviewed 15 smart home inhabitants about their privacy and security attitudes and behaviors. However, our study discussed healthcare and wearable devices in addition to context-aware smart technologies, and involved both users and *non*-users of such technologies.

We audio recorded the interviews and had them professionally transcribed. Three researchers iteratively developed a codebook by independently coding subsets of transcripts and jointly resolving conflicting codes. To maximize the value of thematic analysis, 4 researchers used a holistic coding approach, in which at least 2 coders coded each entire interview, independently selecting excerpts to annotate. All 4 coders then resolved disagreements at the interview level (so that at least 3 out of 4 agreed).

Limitations. We conducted our study in an urban/suburban area with relatively good technology resources, programming,

[1] The interview guide—which also includes questions that will be explored in later papers—can be accessed at https://blues.cs.berkeley.edu/wp-content/uploads/2019/06/Interview-guide.pdf. Entry and exit survey instruments can be accessed at https://blues.cs.berkeley.edu/wp-content/uploads/2019/06/Survey-Instruments.pdf.

and services for older adults, and a relatively high average income due to the high cost of living. Our sample is therefore not fully representative, though it is diverse in terms of level of independence, health, living arrangements, and activity. Because we primarily recruited through senior centers, programs, and living facilities, which often offer computer classes, our participants may be more likely to have attended or at least heard about such classes, and therefore may have more awareness of privacy and security issues. Finally, some participants may have experienced interview fatigue.

4 Participants

Our 46 participants are 65–95 years old (mean=76), 65% female, mainly white (76%), with self-reported native or bilingual English proficiency (45%) or advanced non-native proficiency (37%). They are diverse in terms of income, health, and care situations (Table 1). The majority have an advanced (44%) or Bachelor's (33%) degree. The majority live alone (63%).

Individual characteristics	N	%
Income level		
Less than $35,000	16	35%
$35,001-75,000	16	35%
$75,001-150,000	6	13%
More than $150,000	4	9%
Preferred not to answer	4	9%
Housing		
Independent/assisted living (w/ health facilities)	6	13%
Senior/retirement community	10	22%
Mainstream housing (rent or own)	30	65%
Self-reported health conditions		
Excellent	8	17%
Good	23	50%
Fair	11	24%
Poor	3	7%
Very poor	1	2%
Caregivers		
No one	37	80%
Hired caregiver	4	9%
Informal caregiver	3	7%
Both hired and informal caregivers	2	4%

Table 1: Participant characteristics based on survey responses.

Table 2 shows usage of common devices (11% use none of these). For comparison, 78% of the US general adult population use computers daily or sometimes [7], and 36% use all three [6].

Figure 1 shows participants' self-reported facility with performing certain tasks.[2] Most found basic tasks very easy or somewhat easy. For more advanced tasks, they were more likely to say they had never tried them than to rate them as difficult.

[2]Percentages are out of 45; one participant skipped this question.

Device Type	Daily	Sometimes	Never
Mobile phone, smartphone	52%	22%	26%
Tablet	22%	24%	54%
Computer/laptop	61%	22%	17%
All three	11%	39%	–

Table 2: Device use among participants.

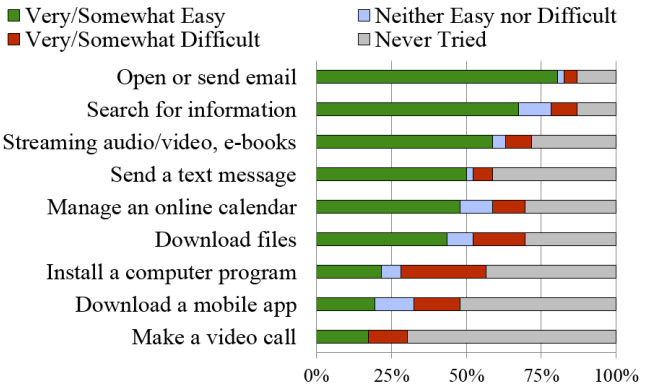

Figure 1: Participants' facility at performing online tasks.

5 Findings

In our interviews, we identified privacy and security concerns (§5.1); mitigation and learning strategies to alleviate privacy and security risks, as well as usability issues with those mitigations (§5.2), and misconceptions about data practices (§5.3). In general, the threat models and associated misconceptions that came up in our interviews are also common among the younger population [cf. 40, 62, 95]. However, we found that, due to infrequent use of technology and limited technical knowledge, health and living situations, financial considerations, and age-related ability declines, older adults may be particularly vulnerable to certain risks, and face more issues with mitigating them.

5.1 Privacy and Security Threat Models

In this subsection, we describe participants' models of perceived privacy and security threats, and discuss how older adults may be particularly vulnerable to certain risks. We found that participants are concerned about the opaqueness of data flows, especially in emerging and unfamiliar technologies. Even if they do not engage with such technologies directly, some still feel exposed to the privacy and security threats those technologies pose (e.g., passive data collection). Privacy choice is particularly limited for residents of senior care facilities.

5.1.1 Taxonomy of Threat Models

Our participants' privacy and security threat models can be categorized in terms of the *activities* that can lead to security and privacy risks, along with the *consequences* of

privacy and security violations. The discussion below follows Solove's taxonomy [81] in dividing harmful activities into 4 types: information collection, information processing, information dissemination, and privacy invasion. We include a comprehensive breakdown of participants' identified threats and concerns, in terms of both harmful activities and harmful consequences, in Appendix A.

Information Collection. One major concern is the lack of transparency about information gathering and people's inability to control it. The issue was raised by 28 out of 46 participants, including 26 who specifically mentioned concerns about collection of data without meaningful notice and consent.

Existing literature has documented the general lack of effective consent mechanisms and transparency regarding data collection practices [78]. This concern is amplified among older adults due to lower technical literacy and experience [85]. For instance, synchronization across devices is a "black box" and source of concern for some participants. Even a participant who volunteers helping others configure devices, considered a computer expert by peers, has trouble tracking it: *"I was concerned that [...] you think you know what shares, but stuff can wind up on another computer so easy with an Apple." "The sharing just surprises me sometimes. You don't know how stuff can go from one to the other, you are surprised it's there."* (P123).

One participant noted that, although data collection by corporations is not new, the Internet and related technologies make collection processes easier, more ubiquitous, and at the same time more opaque: *"The old way, it seemed there was an appearance of consent. [...] Now it's just more seamless,"* (P71).

The inability to control passive audio and video collection by phones and computers—and especially by emerging technologies, like smart TVs, fall detectors, voice assistants, and home-control systems—is of specific concern for 17 participants. Participants believe that information collected by such means may be used for unsolicited marketing, perpetrating physical harm, or violating personal privacy (*"It's scary. Just like, it invades—if the government were to put a microphone in everybody's house and listen to everything you say, people would object. But they are voluntarily putting these devices in their homes and it's doing the same thing,"* P108).

A less common, yet still important, concern participants voiced was about their privacy as bystanders. These concerns were most often related to emerging technologies, such as voice-activated, video-monitoring, and other context-aware systems. Older adults may not be familiar with smart systems, or may even deliberately avoid using them, but nonetheless they are often exposed to data collection by such devices. They may not know how to recognize when smart systems are in use, and may feel uncomfortable about their use by others. This discomfort can contribute to general feelings of helplessness about maintaining control over data collection in the age of ubiquitous computing (*"All my charge cards, all my whatever, everybody knows exactly what I'm doing, even though I never put it on a computer. It's on a computer from someplace else. [...] Every phone call you make is recorded somewhere,"* P43).

Participants often personified data collection processes as though they are conducted by individuals (even when they know it is automated) (*"Whenever you look something up, you get an ad. So a lot of people are reading what you do,"* P5). In some cases, they attributed responsibility for those processes directly to top management: *"The computer [...] probably tracks what you are watching, what you are going to, what you are inquiring about, and keeps a record of it internally. [Interviewer: For what reason?] Because Steve Jobs made it that way. To track data,"* (P69); *"On Facebook, I started—and then they have this Zuckerberg thing about what they were capturing,"* (P104).

Information collection in senior care. Surveillance is another common data collection concern, mentioned by 20 of 46 participants. While a few participants raised broad concerns about government and political surveillance, or referred to personal stalking, the most prominent form of surveillance discussed by older adults was "care surveillance" [30, 68]. Monitoring of older adults by family members, medical staff, or facility management is usually initiated for benign purposes (e.g., to track health status and well-being, or to determine the appropriate level of care). However, such surveillance still induces anxiety, annoyance, and privacy concerns among our elderly participants (*"I know a lot of these devices have cameras in them, and rightly so because they are designed to be helpful, but you know, it's always a concern, I think, when you are using some of the new electronic, is how private are the things that you do,"* P22).

Surveillance is especially common in assisted living facilities or nursing homes. Senior care facilities try to maximize their quality of care and ensure safety while minimizing staff (*"There are sensors so that if you don't go up and go to the bathroom, someone will come down the hall and see if you are okay,"* (P69); *"If [my wife] goes out the front door, it activates a buzzer. There are other residents there who have the same device. [...] The ones that are considered [...] 'exit-seeking,' "* P15). The use of surveillance in care facilities may also be driven by accountability and liability reasons, such as contractual and legal obligations, or to review staff responses to incidents.

Moving to a care facility is often motivated by deteriorating health conditions and the need for a higher level of care. Therefore, older adults living in care facilities are often resigned to giving up privacy in exchange for safety and care (*"You cede a lot of your personal privacy rights when you move into a place like this, in exchange for services being rendered to you. So I think that's a different kind of a setting than somebody that is living in a private setting and would be using devices,"* P71). This finding is consistent with prior literature about tradeoffs between privacy and quality of care [15, 53], and with studies showing positive correlations between the acceptance of privacy risks and deteriorating health conditions [23].

Surveillance is also a concern among seniors who live independently. On the one hand, home care surveillance can

prolong independent living [review in 76]. On the other hand, home care surveillance limits older adults' independence and privacy. Seniors who live independently, and want to protect both health and independence, recognize this tradeoff as a decision they will have to make, if they need more care in the future. As seen in previous research [89], seniors are concerned about how they will balance privacy concerns with the benefits of care surveillance in preserving their autonomy (*"I would probably choose [a wall sensor that detects] presence over having to share a room with somebody being in a nursing home. So if I could stay in my own abode [...] that is a concession that I would make,"* P24).

Information Processing. Almost half of our participants (19 of 46) mentioned aggregation of personal information about individuals from multiple sources, such as web browsing records, smart TVs, and wearable fitness trackers. While some participants find customized recommendations beneficial, most find individual profiling concerning (in some cases both).

However, a few participants showed limited understanding of how inferences can be drawn by combining pieces of data—a blind spot common among younger users as well [2, 63]—or were not certain how much inferencing currently occurs (*"If I were the evil genius, who had that record, I think I could [...] probably tell you more about yourself than you would know about yourself. Or I may be exaggerating, but not too much. [I: Do you believe anyone has the record on you?] I hope not, but, you know... I think most people would find it rather boring, but... [I: Do you think there's some evil genius exists somewhere in the world?] N-n-no, no. This is a hypothetical,"* P51).

Creation of detailed user profiles also enables secondary uses of the data [81], whether by the entity that collects the data or by someone the collector disseminates it to (see below). Our participants are aware of fraud, scams, and identity theft (25/46); targeted advertising (22/48); spam and telemarketing (17/46); and price and service discrimination (7/46). When we asked, "What does that device need to know about you to function properly?" participants' answers often jumped ahead from fulfilling functionality to secondary purposes. For example, when asked what her computer needed to know or collect, P77 responded, *"Cookies. It collects cookies. [I: Okay, what is that?] It tags certain sites that you go into, so the salespeople can send you the right kind of ads, mostly. That's what it says, that what cookies do.."*

In addition to financial fraud and run-of-the-mill online scams like phishing, 3 participants mentioned the potential for fraud on dating websites. This suggests that seniors' engagement with social media and online dating websites—often viewed as mostly relevant to younger generations—should be included in computer training programs for older adults.

Four participants mentioned that fears about information disclosure and/or re-identification limit their willingness to engage in online political discourse (*"I am always chatting about politics and, even on the phone, sometimes I hesitate because I know they cap all that information,"* P46; *"I would do a [Facebook] Like, or submit, and now I've decided not to do that because you just don't know what's being captured. But I really want to support those [political figures]. I don't think we know enough about what's being captured,"* P104).

Moreover, older adults are more engaged in health care activities than the general population [37], which increases their vulnerability to *medical* fraud and scams. Participants generally view medical staff as trustworthy recipients of sensitive personal information and described using online patient portals for managing and exchanging medical information. However, a few participants expressed concern that medical staff may misuse this data (e.g., to assign unnecessary or more expensive treatments, or for personal retaliation). Misuse can have severe consequences (*"I got a bill from the hospital for $26,000. They had padded it. [...] I can't prove that none of that stuff happened,"* P5).

Insecurity resulting from inadequate protections is another frequent concern. Twenty-four participants mentioned hacking, and six specifically mentioned viruses or malware.

Information Dissemination. With regard to information dissemination, older adults were primarily concerned with their personal information being sold for profit, or being disclosed with malicious intent to cause reputational damage, humiliation, or embarrassment.

Specifically, 11 participants discussed the possibility of information being sold and subsequently used for secondary or even malicious purposes (*"If it's confidential and private, I don't care if they have all my information. [...] As long as [...] it wouldn't be abused, or I'd get a bunch of salesmen calling me trying to sell a device or a pill or something,"* P10). Others' concerns were more general (*"I would just like to see some kind of safeguard [...] in the technology so that strangers [...] don't have access to knowing everything about you, because strangers don't really need to know,"* P47). Even if the initial intent is not malicious, disclosure of sensitive economic and health information can endanger benefits older adults might otherwise receive, such as social security, disability allowance, insurance coverage, and eligibility for senior housing or assisted living facilities.

Participants concerned about scams and fraud often recognized that the information being used by scammers (or even hackers) for illegitimate purposes may come originally from disclosures someone purposely made to legitimate recipients, demonstrating again the limits of users' control (*"I no doubt shared my social security number with some other benevolent entity [...] but that someone decided that that might be of value in the open market,"* P51).

Unlike with commercial data, in the few cases where participants mentioned specific cases of medical data having been shared in ways they saw as violating their privacy, it was usually obvious to them who had shared it and when.

However, participants also expressed the desire to balance

privacy and security with the benefits of data portability, especially with regards to healthcare, research accessibility, and legitimate access delegation (*"I wish [doctors] would share [my medical records with each other], but they don't. It's so compartmentalized that it's [...] really frustrating. [...] It's a benefit and it's a curse, [...] because [...] unless you tell them, [...] they don't know what is going on with the [other] doctors in your life,"* P46). For instance, the poorly defined legal role of informal caregivers generates annoyance about privacy and security protections and may erode privacy values (*"The privacy to me seems like overkill. The concern about the hoops I have to jump through to be able to order the wife's prescription or to speak for her. I know that there are lawsuit reasons [...] so they have to be so so so so careful. But I don't share that concern. It probably shows that I am naïve,"* P123).

Privacy Invasion. While the risks of physical attacks and reputation damage are not exclusive to the online world, participants noted that modern technology exacerbates them (*"When you are having a private discussion with someone, you ought to be able to feel that it's as private as those that are involved in it are willing to be, you know. You can't obviously be sure that they won't go blabbing it all to the next person they talk to, but, I wouldn't want technology doing that for me,"* P15). Participants were particularly concerned about location data and data about their in-home activities, which some saw as sources of compromising information that could facilitate physical attacks on them or their property.

A few of our participants were also concerned about interference in their decisions, such as the use of social media to interfere in the US elections (*"I think that they expected that Facebook information would be effective in addressing specific group of voters. When you think about it, it is not far-fetched. It is perfectly reasonable,"* P121).

5.1.2 Seniors' Views About Age-Based Differences

Some participants discussed beliefs about generational differences in privacy attitudes, or in privacy risks.

Beliefs about Whether Seniors Are More Concerned about Privacy than Younger People. We observed a dichotomy in seniors' views on age-based differences in privacy attitudes. Some participants (9/46) expressed fundamental beliefs about privacy. They explained that they grew up with the idea of privacy as a valuable human right, where information sharing has limits and rules defined by social norms—norms that some believe are changing across generations (*"...People say, 'Well, if you've got nothing to hide, why don't you tell them?' It's none of their business! [...] It's much less so in this new age: the millennials, they don't seem to be quite so concerned about it. But when I was growing up there was some very strong limitations on what you ask people, what you told people. [...] So it's a generational thing,"* P22).

Some other participants (4/46) expressed the contrasting belief that older adults do not need to worry about privacy as much as younger people do. Some ascribed particular reasons, such as not being concerned about job opportunities (*"If I was younger, it might hinder me from jobs or even benefits of some kind. But now I don't think it would inhibit me from benefits,"* P21).

So while some described changing needs or views over time (*"This may be a function of age because, at this stage of my life, I don't feel like I have great secrets or private information,"* P6), others view privacy as a constant (*"I'm old fashioned enough to know what privacy is and to value it. [...] If at my age I don't have a few things to hide from a few people, my life has been totally wasted,"* P113).

Beliefs about Whether Seniors Are Seen as Attractive Targets. Participants expressed some contradictory opinions about whether older adults are viewed as better targets for security and privacy attacks. Several participants believe older adults are specifically targeted because they are viewed (correctly or incorrectly) as vulnerable, easy targets, especially for social-engineering attacks. They attribute the targeting to assumptions about seniors' low technical literacy; lack of support (*"I think [they falsified bill] because they think old people are stupid or they're not aware and I was there alone. I couldn't prove anything,"* P5); or gullibility (*"Because it's elderly are more fallible, or they're more trusting, so they take advantage,"* P7). At least one believes attackers make assumptions about their financial situation (*"Maybe he thinks I'm wealthy and [is] after my money,"* P13).

In contrast, a few older adults believe that attackers do not see them as "major consumers" (P110) and doubt that their information is useful enough to be exploited for commercial purposes (*"I think that I am not a focus of whatever these companies are looking for. They probably look at my data—if they look at it—and say, Oh, don't bother with her. She's too old to participate, or maybe doesn't have enough money, or I don't know what they think,"* P110).

5.1.3 Unrecognized Threats

Some older adults in our interviews did not purchase their own devices, and instead rely on used devices or public equipment and services. Few of those participants mentioned potential privacy and security threats associated with public or used devices, which we discuss below.

Use of Public Devices and Services. Older adults are less likely to own their own computers or smartphones than younger people [7], therefore, seniors are more likely to use public devices. Six participants mentioned that they use public computers (e.g., in libraries or at senior centers). Some use public medical devices; two participants mentioned that because they do not have blood pressure monitors at home, they *"go to Walgreens and other places, where they have free*

checks. And I got it checked recently at a health fair," (P10). Privacy and security in such situations depends on what data is collected, how it is stored and used, and whether the devices and entities collecting it are subject to HIPAA [61].

Participants' use of public devices is usually motivated by either the high cost of purchasing a device or a lack of perceived utility in owning one, e.g., due to infrequent use. Infrequent use in turn amplifies security risks related to lack of skills and experience, e.g., in detecting malicious events or suspicious websites, links, or documents [71–73].

Only few participants expressed concerns about public devices or public Wi-Fi networks, even though they are more likely to expose users to vulnerabilities such as malware infection, data leaks, and other privacy and security threats resulting from accidental shared access, shoulder surfing, and Wi-Fi spoofing. Instead, most simply appreciated that someone else was maintaining the devices: *"That's another reason why I don't want a home computer. I go to the library, and if [the computers there] crash, they'll deal with it. [...] If I had one, and it crashed [...] I'd just leave it off. I don't want to have to pay for the repairs,"* P10. However, the effectiveness of maintenance is a function of the expertise and diligence of the person in charge and of the resources available at the public facility. Moreover, the security efforts of administrators can still be compromised by user behavior [9].

Use of Second-Hand Devices. Seven participants mentioned that they use second-hand devices given to them by family, friends, or neighbors (*"Grandpa gets the oldest phone. When they get upgraded, the phones trickle down. [...] I am thrilled with it, and it is too old for anyone else to use in that household,"* P121). The most common were smartphones, computers, tablets, and TVs, though one person mentioned a cleaning robot. Refurbished computers were also mentioned.

Reuse of such devices entails serious security and privacy risks, for both the previous owner (e.g., personal data disclosure, unauthorized access) and the new owner (e.g., malware and viruses). Moreover, access to technical support and security updates declines over time, further increasing vulnerability [70]. However, no older adults among our participants mentioned any potential risks from using second-hand devices, and only one mentioned that the previous owner reset the device, although it is not clear how effectively it was done (*"My friend did give me her old Mac. So I need to set that up. She wiped hers out. It's an older one, but she was using it for school, and she did video chats and everything on it, so it's very up-to-date. I don't need the latest,"* P36).

5.2 How Older Adults Manage Privacy and Security Risks

Similar to previous studies with older adults [16, 36, 47], our participants hold a range of attitudes about whether privacy and security concerns can be addressed in the current environment—which affects their attempts to mitigate those concerns. Some participants were pessimistic, believing that users have lost control over their personal information (*"I wish they would take the word privacy out of the dictionary. There is no such thing anymore. [...] I think it's the genie out of the box. I don't think it can be addressed,"* P43).

Such fatalism can result from a perceived lack of control and transparency, which leads to inertia against taking active security- and privacy-enhancing steps (*"I was thinking of cancelling my Facebook account but then I read that even if you're not a member, that they can get all kinds of information, so I don't know if I want to bother with that,"* P20). Another reason is a lack of confidence about having the knowledge and skills to protect one's own information (*"I'm not sophisticated when it comes to all these electronic gadgets and so I don't know what the possibilities are for control that is unavailable to hackers and thieves,"* P20).

Some participants explicitly attributed their attitudes to age (*"Don't forget, I'm old. And some things [...] you just sort of have to let go and you don't want to use your energy at it. [...] I want my information back and they say no, sometimes you just have to go ahead [...] Not everybody can fix everything. You just have to live with the consequences. That's why you shouldn't be saying nasty things on the Internet, because it comes back to haunt you and you can't fix them,"* P107).

Other participants are less fatalistic and discuss how privacy can or should be restored and protected (*"I value privacy. I don't necessarily want anyone who wants information about me to be able to get it too easily, and too cheaply. If they are going to get it, I want them to work for it, and pay for it, as a way of discouraging them,"* P113).

5.2.1 Passive and Active Mitigation Strategies

We categorize the end-user security and privacy management strategies participants talked about along a scale of *passive* to *active* approaches.

One of the most commonly mentioned (28/46) passive mitigation strategies is to limit the use of technology or to avoid it altogether—sometimes causing notable inconvenience to the non-user (*"When you get Uber, if you don't log out and sign off each time, they know where you are all the time. I don't like that, location. [...] [I: So, what are you doing about that, do you still use Uber?] No, I don't. [...] It is just that when I go [...] in the city, instead of getting on the bus it is easier call Uber and, you know, but I have discontinued that,"* P46).

Other passive strategies include using services and devices with good reputations or brand image, and just generally trying to be cautious. Relying on such passive strategies is a double-edged sword. For example, relying on caution is subject to overconfidence bias [1], and depends on the user's vigilance, knowledge, and skills in detecting malicious actions and predicting the consequences of their behavior [18]. At the same time, unfortunately, many participants mentioned simply

accepting or ignoring known risks.

Active mitigation strategies include configuring privacy and authentication settings, using protective software and services, and deleting or refusing to provide personal information. Many participants mentioned strategies that mitigated the consequences of violations rather than the causes, such as blocking unwanted contacts or content, or discontinuing their use of devices or services after experiencing privacy or security violations. We provide more details about these strategies, along with supporting quotes, in Appendix B.

5.2.2 The Role of Usability and Learnability

Our participants often explicitly view themselves as vulnerable to privacy and security threats because they have trouble using and configuring new technologies by themselves and/or because they know less about how the technologies work.

Usability, Learnability, and Risk. Participants mentioned obstacles related to the usability and learnability of privacy and security functions. These obstacles often result from or are amplified by general usability issues.

Despite their prevalence, passwords suffer from well-known usability issues [66, 84, 93], such as needing to be memorized and changed (*"I have a list of [passwords], and sometimes the computer will remember them, which is helpful, and then sometimes not. I have it written down and sometimes they make you change the password and I forget to write it down,"* P6). Participants have a variety of strategies for dealing with this—including strategies that are commonly viewed as poor security practice (re-using, choosing simple/guessable passwords). Many participants have heard advice about good password practices, but cannot effectively implement all of that (sometimes conflicting) advice (*"I use the same password for everything and I have used the same password for years. Even though we have been advised not to do that. [...] It's hard enough for me to come up with a password that I can remember and not write down—they tell you not to write it down so I don't do that,"* P110).

In addition to authentication, participants mentioned potentially privacy-relevant usability issues like accidentally activating voice control on a phone, or not being able to figure out how to sync email to delete a message on all devices at once. In addition to a general feeling of having lost control or not having mechanisms to exert it, several participants doubt such mechanisms could ever be usable (*I: "What if the system will give you control over the information so you can decide who can access it? [...]" P: "That's just too much trouble. [...] By observing other people with computers, they are always messing up. [...] It's not just push a button and have it do what you want,"* P1).

Delegation of Privacy and Security Management. A related issue is that older adults often involve others in managing their privacy and security (e.g., configuring settings) [cf. 70]. They may even hand it over completely to family members, someone in their community, or technical experts (*"It's called Touch ID? [...] Yeah, I think I've heard of that, but my son did not set me up for that,"* P103). Delegation of security maintenance is a common practice among the general user population [29, 32], but due to especially limited digital literacy and experience, it may occur more frequently among senior users [12].

Older adults' need to turn to others for help with non-security-related technical issues (e.g., general setup and maintenance) can have security consequences. (Table 6 provides a general overview of older adults' tech troubleshooting strategies and issues that arise with each.) For example, sometimes older adults share account credentials with family members, friends, and (professional or volunteer) technical assistants [94]. One such community "technical assistant" commented: *"She didn't mind if I put [her] Amazon account in [my] phone, the credit cards and stuff, but I didn't want to get my Amazon account confused with hers, that's for sure,"* P123.

The Consequences of Delegation for Learning. Although relying on relatives and acquaintances to take care of technology setup and maintenance works for some participants, others discussed the difficulties such reliance can create. In particular, children or other family members might not have enough time to help, or when they do, might try to forestall further needs by discouraging older adults from fully using the technology. Limited explanations may leave older adults with an awareness of risks but few details on how they come about (*"My son is very good protect for my computer, not everybody can get it. It's very security for that. He just don't want me to check this, check that, get a virus. [I: So how does he protect...?] I don't know,"* P16). These issues emphasize the need for older adults to have independent channels for learning about and troubleshooting technology.

A few participants acknowledged explicitly that relying on others to set up and troubleshoot devices means they don't have much understanding about how they work (*"It's just part of my resistance to technology. [...] [The paid technician] is a smart guy and I don't have the patience to unravel it if it is not doing what it is supposed to do,"* P8).

A few said they just aren't interested in learning (*"I kind of just decided that I'm not interested in learning a lot of new technology,"* P77), but even those who are interested can find themselves falling back on asking others to solve problems for them (*"I belong to the computer club. [...] I've gone to their picnics a couple of times, but if you belonged to the club you have someone that will come and help you if you have problems with your computer. I don't have to know that much about it if I have a problem,"* P5).

5.2.3 Sources of Information on Risks and Mitigation

Even participants who had not been targeted for specific privacy or security attacks seemed generally aware of potential

issues and described sources where they learned about risks.

News media are a common source [cf. 70]. Given the timing of the interviews (May–June 2018), Facebook's Cambridge Analytica scandal [13] came up frequently (*"Judging from the recent things that have come out with Facebook and Mark [Zuckerberg], I realize that whatever you type in, goes out"* P32). Several participants mentioned having heard about Alexa mistakenly sending a private conversation to a random contact in the owner's address book [46], as well as other stories about identity theft, data breaches, and data brokering.

Stories are sometimes accompanied by tips on how to avoid such scams or mitigate consequences of larger incidents, especially in publications for seniors such as the *AARP Bulletin* (*"Sometimes when [the service provider says], 'You should change your password. Your identity may have been stolen,' or something like that, then I would change my password. [...] Or, you know, on TV they would make that suggestion,"* P13). Data breach notifications from companies did not feature prominently in our interviews.

When the mitigation against a particular incident is fairly simple, these channels seem effective. However, more general or more complicated stories sometimes leave participants confused about the actual pathways data can take, and with a garbled or incomplete idea of how to protect themselves (*"Well I read in the paper that there are these search engines and they can get into computers [...] especially through Wi-Fi so I have Wi-Fi turned off,"* P108).

Another source of information about risks and mitigations is materials, classes, or lectures targeted specifically at older adults. Computer classes we saw advertised for seniors contained some privacy and security content. Generally, participants find computer classes beneficial (*"They give lessons, many, many classes every year on how to use your phone, or how to use computers, or how to use anything [...] and they're very good,"* P5). However, some noted that *"it's hard to know if [classes are] at the level that you need"* (P18), or find classes too difficult (*"I need like ABCs, 1-2-3s. It was not basic enough for me,"* P69).

Several participants mentioned having attended or heard about talks on how to avoid scams. For those classes, the relevance is generally clear (*"They have seminars on [...] how to avoid being scammed. [...] [I: Do you believe that it could happen to you too?] Yeah, why not, sure, but..."* P7). But in other cases, participants did not make the connection between lecture content and consequences for their data (*"Somebody came and talked about the cloud. What is it, what does it do, you know, that kind of thing. I went and I thought I don't need all this. [...] I just look things up and send a few emails and that's about it. I don't care about anything else,"* P5).

5.3 Notable Misconceptions and Blind Spots

We identified common misconceptions regarding technology, data collection and sharing, and protections that could lead to older adults' forming inaccurate privacy and security threat models, or increase their vulnerability to risks.

5.3.1 Uncertainty about Information Flows

Uncertainties about what data is collected, transferred, and used, and how, are common in the general population [8, 62, 90], and among our participants in particular. In addition to lack of transparency about data practices, lower technical awareness and experience can aggravate the proliferation of such misconceptions among the elderly.

As noted in §5.1.1, some participants expressed incorrect assumptions that technology only collects information users input themselves, or were uncertain about it (*"I like to think that the smartphone only has in it what I put in it. Now I could be dead wrong but I like to think that,"* P22; *"I don't see my phone capturing my data, unless—what I enter,"* P104).

In contrast, some assume that virtually everything is collected, shared, and retained, which can lead to fatalism or resignation (*"Apparently they can track, from cell phones and cell phone towers they have a record, they can piece together so much about you,"* P113).

In a couple of cases, misconceptions about data collection were due to uncertainty about which devices are Internet-enabled (*"I am assuming that [a smart speaker] is not really connected to the Internet. It has to do with information you put in, so I wouldn't worry about what information they had about me. [...] [I: It is connected to the Internet.] [...] Okay well I am wrong then, then it will know a lot more,"* P46). However, it was rarely so clear whether our respondents thought data collection and processing happen on-device or whether it is sent off-device. Although studies have shown [50] that this is an important distinction for users when asked about it explicitly, our study participants did not specify it unprompted.

Data flows in emerging technologies are especially opaque for older adults because they may be less familiar with the state-of-the-art sensors and algorithms, or with advances in artificial intelligence, than the younger population [80]. They may base their assumptions about how devices work—and therefore their privacy mitigations—on analogies with more familiar technology (*I: "What kind of information would you expect the devices to collect about you? [...] What about the smart speaker?" P: "Answering questions. I have begun to use this feature in the phone. [...] So, I guess what the smart speaker would do would be anything that the smart phone can do and then maybe more. I don't know what that might be,"* P60)—[cf. 69].

5.3.2 Uncertainty about Data Persistence

We also identified misconceptions about the effectiveness and extent of data deletion. A couple of participants said that when they delete a file or an email, they believe there is no longer any record of it, while in practice it is still locally stored and was simply moved to a Trash folder. The feedback they receive

from synced devices (when working correctly) reinforces this belief: when email is deleted on a computer, you can no longer see it on a mobile device, suggesting that it was deleted permanently (*"It is all connected. Once I delete it [on the computer], the phone is also,"* P7).

Several participants believe that data is overwritten, rather than stored permanently on the device or in a digital database. Sometimes these assumptions are based on analogies with older or more familiar technologies (*"I thought it was just [...] like recording over the tape [...] like where you used to tape programs from television. If you recorded over that tape, you wiped out pretty much what had been said or done,"* P35).

A couple of participants were also surprised about the duration of data retention (*"I hadn't even thought about [hearing aid apps] collecting [data], or where all that stuff goes. I think it's only me hearing it. Phew. Is a record of that around forever?"* P123).

Some participants assume that the information a device shows the user is a complete record of everything that device has collected (*"There's nothing that is recorded. [...] The only thing the phone would show is who called me,"* P110).

5.3.3 Blind Spots in Mitigation Strategies

Beyond data deletion, misconceptions about data flows and persistence, or about security mechanisms, may lead to older adults relying on other ineffective means of protection, or using protection strategies ineffectively.

Several participants mentioned not being sure about the effectiveness of their strategies (*"I gave money to a firm that said that they would provide some protection for my bank account, brokerage account. I don't know whether really that they would be that effective. [...] Probably a waste,"* P51). In extreme cases, the "security service" turned out to be a scam or ransomware attack (*"I got a call from some outfit that said that there was [...] some billing that had been done on my account from Russia. [...] And I said I didn't order that. [...] They persuaded me, which was an error on my part, to buy some service from them, and I bought the service and then I was told that that service offering was a scam,"* P20).

In contrast, some other participants may be overly confident about the effectiveness of the mitigation strategies they use, or due to lack of knowledge, consider less technologically advanced threat models. Such overconfidence may lead to neglecting security advice or reducing protection efforts: *"The nice thing about using Apple, is that there aren't hackers like there are with Windows. In Windows everything gets hacked so you have to have an anti-virus, an anti-something else, and you have to have the firewall. My Mac has two firewalls and that is all I need. [...] I think they come installed,"* P25).

Even when participants were aware of threats, they often did not know how to effectively protect against them. For example, P22 said *"I try to change my passwords regularly. And a lot of my passwords are so obscure I would be surprised if anybody could figure them out, although I know that they can be figured out. The references in my passwords are to things that nobody would associate with me. [...] So that's how I try and protect myself. I don't know how else to do it."* When choosing passwords, she does her best to try to make it harder for a lay person, presumably knowing some basic information about her, to guess it. However, such passwords may not be at all "obscure" for a hacker using brute force.

As we noted in §5.2.1, several participants mentioned strategies that mitigate privacy and security consequences, rather than the risks themselves. In some cases, they do not necessarily recognize that these strategies do not address the causes of the threat—or are not concerned that they do not. For example, a participant mentioned blocking telemarketing calls (*"I also have a call blocker on my phone. So I got rid of those unwanted calls [and] robocalls,"* P110). The participant was satisfied with the strategy, but of course a call blocker does not remove personal information from call lists.

A few participants acknowledged the ineffectiveness of mitigating consequences in addressing root causes, but said they felt helpless to find a better solution (*"You lose control once some outside agency has information. I am unable to stop the flood of phone calls whose origin and purpose I cannot imagine. The only thing I can do is what one daughter-in-law suggested—don't answer it,"* P69).

Unsubscribing, discontinuing, or simply abandoning a service can be as ineffective in addressing the root cause of the risk as mitigation of consequences. And when not done properly, it may even increase exposure. For example, abandoned accounts are often used for social engineering attacks and identity theft [88] (*"The other [incident of identity theft] almost had to be dishonest people that can view credit bureaus. Because a couple of accounts that we had zero balance on, we had cut up the credit cards, we had not closed the accounts,"* P123).

Finally, users only employ mitigation strategies when they have some awareness of the risks. Infrequently recognized risks are therefore infrequently protected against, for example, risks associated with public or hand-me-down devices (see §5.1.3).

5.3.4 Belief They Have Nothing to Hide

Echoing the "nothing to hide" fallacy [82], many participants feel that an honest person who has nothing to hide should not need to protect their privacy (*"I have no nefarious activities, so I have no problem,"* P121; *"I'm not that sensitive. I'm very 'open book' person,"* P31).

Similarly, some participants do not recognize the potential risks of data misuse (or underestimate its probability) if they do not view the information as sensitive or high-value (*"Who would really care how many steps a day I take? [...] I can't see how anybody could use that information to make money. [...] Unless maybe they wanted to sell me some exercise equipment, like a treadmill. [...] I don't see that as a realistic possibility of ever happening,"* P7).

One possible explanation for why these misconceptions occur is that participants often focus on the considerations of potential reputation damage and overlook broader security risks that could lead to material and financial consequences, or threats to physical safety. Although not unique to the older population [82], this misconception was quite common in our interviews, so we believe it is important to consider when designing privacy and security interventions for older adults.

6 Discussion and Implications

Below we summarize our findings, then use them as a basis for recommendations to providers of security awareness programs and education, and to technology designers. We also discuss potential future work.

6.1 Recap of Main Findings

Comparative findings in prior work show that distribution of privacy and security attitudes is similar across age groups [40, 41, 62, 91, 95], while privacy and security knowledge, behaviors, and risk levels differ [e.g., 34, 36, 41, 48, 58, 62, 73, 90]. Our results add depth to this picture, illustrating how certain privacy and security risks are amplified for older adults.

Amplification can be due to less knowledge and experience with technologies, decline in physical and mental abilities, and/or specific financial or living situations. For instance, we found that inhabitants of senior living facilities are particularly subject to surveillance, and often have to give up privacy and control of personal data. Our participants often reported using public and secondhand devices and public Internet access, yet they are not always aware of the potential threats involved. They are also concerned, confused, and often have misconceptions about data flows and risk mitigation strategies.

Participants provided insights on barriers to learning about, understanding, and using privacy and security protections, which are heightened by memory decline and physical limitations. In particular, we find that difficulty in using technology—whether older adults attribute it to user-unfriendliness or to their own lack of skill or knowledge—leads to a lack of self-efficacy about privacy and security. Therefore, addressing those barriers is an important basis for empowering older adults to use technology more safely and comfortably.

6.2 Suggestions for Awareness and Education Programs

We found that many older adults lack a nuanced understanding of newer technologies and the data they collect, leaving them especially vulnerable to privacy and security violations. Their particular concerns, misconceptions, and blind spots could be addressed through tailored training and educational efforts.

Expand educational programming. Existing programming that older adults find valuable, such as computer classes, lecture series, or computer clubs, can be expanded. We recommend developing security and privacy materials *specifically designed for this age group*, in collaboration with trainers and older adults themselves. In addition to scams, such materials should address issues of most concern to older adults, such as surveillance, and misconceptions about data collection, persistence, and sharing. Engagement in social media, including dating websites, should not be overlooked. Potential risks of using public or hand-me-down devices, and how to mitigate them, should also be considered.

Targeted materials will allow those leading the classes to more easily tailor them to seniors' needs and knowledge—including making the necessary connections between technical facts and practical consequences, so that seniors better understand the relevance of the technical details.

Leverage existing points of contact for outreach. Privacy and security information for older adults can be disseminated via channels they already use to get help with computer problems (see Appendix C), as well as resources they look to for general help and advice, such as publications or websites directed at seniors [cf. 70].Vendors and computer-repair experts could make age-appropriate privacy and security "checkups" a standard part of setup or troubleshooting conversations with seniors.

6.3 Suggestions for Technology Developers

Participants often avoided or stopped using technology due to privacy and security concerns or violations, which also affect their intentions to purchase and use emerging technologies. Participants frequently linked their privacy and security behaviors to usability concerns. This finding is an important illustration of the direct economic incentive for technology designers, developers, and manufacturers to address the privacy and security concerns of older adults.

Improve transparency and control, address misconceptions. Security and privacy controls should be designed to account for misconceptions common among older adults (see §5.3), to anticipate and address respective risks. Incorporating privacy controls *where the default is the most private setting*, as older adults rarely configure them [42], is a first, basic structural change.

Standardizing and being upfront about the types, amount, and granularity of information collected and shared may enhance older adults' awareness and reduce the likelihood they will discontinue use after being surprised by a perceived privacy violation. Device descriptions and apps should make clear when information is sent over the Internet (rather than processed on-device), and where possible should incorporate data-transmission indicators [38, 55, 100].

Address usability issues and improve system design. Interfaces should be designed to optimize older users' ability to authenticate, configure settings, and accomplish other security tasks without errors in a reasonable time. For instance,

usability issues associated with aging-related ability declines, such as reduced vision and acuity, hand tremors, memory worsening, and lower skin conductance [17], may complicate authentication management [33] and may lead older adults to choose less secure mechanisms.

To address the identified usability issues, designers can rely on expansive knowledge and guidelines in that area [25]. For instance, they can add security indicators for "trustworthy" applications, or provide default configurations for data backup [21]. Designers and developers should focus on facilitating information management (e.g., editing and deleting personal records). Companies should involve older adults in the development process through participatory design and usability testing.

6.4 Future Work

Some of the patterns we identified in our exploratory qualitative study merit further systematic investigation, such as older adults' uncertainties about data deletion and retention, or their use of public and secondhand devices. Consequences of those behaviors could be assessed in controlled behavioral studies. In particular, it is not yet clear how the issues we identified affect older adults' privacy and security behavior as compared to the general population, or whether their security and privacy management strategies are more or less effective than those of the general population.

Older adults' use of emerging technologies, especially healthcare technologies, also warrants further exploration. While many of our participants used such technologies, or had heard of them, their use and knowledge was sufficiently heterogeneous that clear themes did not emerge. Further research is needed to examine specific privacy and security questions about older adults' use of these technologies in greater depth and at larger scale.

Finally, the measures we recommend should be tested "in the wild" to determine their efficacy. For example, we might test whether having targeted training materials for educational programs can positively impact older adults' privacy and security behaviors; or whether more transparency about data collection and sharing improves their comfort with using an app or device. Of particular importance would be age-specific usability tests of enhanced privacy and security controls, especially for new types of technologies such as healthcare and other monitoring devices.

7 Conclusions

As the population of older adults grows and turns their attention to technology, systems will need to be designed to enable informed choices, better control over personal data, and improved security for this user group.

Through semi-structured interviews with 46 older adults, we identified a variety of privacy and security attitudes and concerns, threat models and mitigation strategies, common misconceptions, and usability issues with currently deployed privacy and security controls. In general, the range of privacy and security attitudes, as well as the threat models and associated misconceptions mentioned by older adults in our interviews and reported in prior research, are also common among the younger population. However, our findings illustrate how older adults may be *particularly vulnerable* to certain risks and experience difficulties in mitigating them, due to age-related declines in abilities, and to their relative lack of technical knowledge and experience (shown in previous studies and confirmed here).

Emerging technologies featuring smart sensors or machine learning algorithms were especially concerning for our participants. Their data flows were difficult for participants to understand, likely because of their opacity. Participants specifically mentioned concerns about passive data collection (e.g., by smart speakers) and their privacy as bystanders (when other people's devices collect information about them).

Our participants often reported using public and secondhand devices and public Internet access, but were not always aware of associated privacy and security risks. They also mentioned concerns over the disclosure of sensitive financial and health conditions, which could be accelerated by the proliferation of e-health and health-monitoring systems. Participants mentioned concerns that such disclosures may endanger benefits they might otherwise receive, such as social security, disability allowance, insurance coverage, or eligibility for senior housing or assisted living facilities.

Residents of senior care facilities especially often acknowledged being resigned to the loss of privacy in exchange for care and safety. For seniors living independently, balancing the tradeoffs between care/safety and privacy is an open dilemma, as it conflicts with their desire for independence.

Finally, we found that one of the most commonly mentioned approaches to mitigating privacy and security risks was to avoid or limit using the technologies. This finding suggests that businesses offering devices or services targeted to or used by older adults may accrue economic benefits and gain a competitive advantage by considering the opinions and addressing the concerns of this population.

Acknowledgments

CHI workshop participants provided helpful comments about the study, as did anonymous CHI and SOUPS reviewers. We also thank our participants, and Joy Qiaoying Tang and the organizations that assisted in recruitment.

This work was supported by generous gifts from Cisco and Mozilla, by a grant from the Center for Long-Term Cybersecurity (CLTC) at U.C. Berkeley, by National Science Foundation grants CNS-1514211 and CNS-1528070, by the National Security Agency's Science of Security program, and by the Rose Foundation for Communities and the Environment. Opinions, findings, and conclusions are those of the authors and do not necessarily reflect the views of the funders.

References

[1] A. Acquisti, I. Adjerid, R. Balebako, L. Brandimarte, L. F. Cranor, S. Komanduri, P. G. Leon, N. Sadeh, F. Schaub, M. Sleeper, et al. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)*, 50(3):44, 2017.

[2] A. Acquisti and R. Gross. Predicting social security numbers from public data. *Proceedings of the National Academy of Sciences*, 106(27):10975–10980, 2009.

[3] Ageless Innovation LLC. Joy For All Companion Pets, 2018. https://joyforall.com.

[4] I. Altman. *The Environment and Social Behaviour: Privacy, Personal Space, Territory, and Crowding*. Brooks/Cole Publishing Company, 1975.

[5] K. B. Anderson. *Consumer fraud in the United States: An FTC survey*. Federal Trade Commission, 2004.

[6] M. Anderson. Smartphone, computer, or tablet? 36% of americans own all three. Technical report, Pew Research Center, 2015.

[7] M. Anderson and A. Perrin. Technology use among seniors. Technical report, Pew Research Center for Internet & Technology, Washington, DC, 2017.

[8] C. M. Angst and R. Agarwal. Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly*, 33(2):339–370, 2009.

[9] M. Arora, K. K. Sharma, and S. Chauhan. Cyber crime combating using KeyLog Detector tool. *International Journal of Recent Research Aspects*, 3(2):1–5, 2016.

[10] I. Azimi, A. M. Rahmani, P. Liljeberg, and H. Tenhunen. Internet of Things for remote elderly monitoring: A study from user-centered perspective. *Journal of Ambient Intelligence and Humanized Computing*, 8:273–289, 2016.

[11] S. Beach, R. Schulz, J. Downs, J. Matthews, B. Barron, and K. Seelman. 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):5:1–5:21, 2009.

[12] V. Boothroyd. *Older Adults' Perceptions of Online Risk*. PhD thesis, Carleton University, 2014.

[13] C. Cadwaller and E. Graham-Harrison. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*, 2018. Accessed on 19 September 2018.

[14] K. E. Caine, C. Y. Zimmerman, Z. Schall-Zimmerman, W. R. Hazlewood, L. J. Camp, K. H. Connelly, L. L. Huber, and K. Shankar. DigiSwitch: A device to allow older adults to monitor and direct the collection and transmission of health information collected at home. *Journal of Medical Systems*, 35:1181–1195, 2011.

[15] R. M. Califf and L. H. Muhlbaier. Health Insurance Portability and Accountability Act (HIPAA): Must there be a trade-off between privacy and quality of health care, or can we advance both? *Circulation*, 108(8):915–918, 2003.

[16] J. Camp and K. Connelly. Beyond consent: Privacy in ubiquitous computing (ubicomp). *Digital Privacy: Theory, Technologies, and Practices*, pages 327–343, 2008.

[17] N. Caprani, N. E. O'Connor, and C. Gurrin. Touch screens for the older user. In *Assistive technologies*. InTech, 2012.

[18] E. L. Carlson. Phishing for elderly victims: as the elderly migrate to the internet fraudulent schemes targeting them follow. *Elder Law Journal*, 14:423, 2006.

[19] B. Carpenter and S. Buday. Computer use among older adults in a naturally occurring retirement community. *Computers in Human Behavior*, 23(6):3012–3024, 2007.

[20] Cherry Home. https://cherryhome.ai, 2018. Accessed on 14 September 2018.

[21] E. Chin, A. P. Felt, V. Sekar, and D. Wagner. Measuring user confidence in smartphone security and privacy. In *Proceedings of the 8th Symposium on Usable Privacy and Security (SOUPS)*, page 1. ACM, 2012.

[22] J. Chung, G. Demiris, and H. Thompson. Ethical considerations regarding the use of smart home technologies for older adults: An integrative review. *Annual Review of Nursing Research*, 34:155–181, 2016.

[23] J. F. Coughlin, L. A. D'Ambrosio, B. Reimer, and M. R. Pratt. Older adult perceptions of smart home technologies: Implications for research, policy & market innovations in healthcare. In *29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pages 1810–1815. IEEE, 2007.

[24] L. Coventry and P. Briggs. Mobile technology for older adults: Protector, motivator or threat? In J. Zhou and G. Salvendy, editors, *Human Aspects of IT for the Aged Population. Design for Aging*, pages 424–434, Cham, 2016. Springer International Publishing.

[25] S. J. Czaja, W. A. Rogers, A. D. Fisk, N. Charness, and J. Sharit. *Designing for Older Adults: Principles and Creative Human Factors Approaches*. CRC Press, 2009.

[26] G. Demiris, D. Oliver, G. Dickey, M. Skubic, and M. Rantz. Findings from a participatory evaluation of a smart home application for older adults. *Technology and Health Care: Official Journal of the European Society for Engineering and Medicine*, 16:111–8, 2008.

[27] M. Di Rosa, V. Stara, L. Rossi, F. Breuil, E. Reixach, J. G. Paredes, and S. Burkard. A wireless sensor insole to collect and analyse gait data in real environment: The WIISEL project. In B. Andò, P. Siciliano, V. Marletta, and A. Monteriù, editors, *Ambient Assisted Living: Italian Forum 2014*, pages 71–80. Springer International Publishing, Cham, 2015.

[28] K. Dobransky and E. Hargittai. Unrealized potential: Exploring the digital disability divide. *Poetics*,

58:18–28, 2016.

[29] P. Dourish, E. Grinter, J. Delgado De La Flor, and M. Joseph. Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, 8(6):391–401, 2004.

[30] A. Essén. 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):128–136, 2008.

[31] S. Fang, Y. Liang, and K. Chiu. Developing a mobile phone-based fall detection system on Android platform. In *2012 Computing, Communications and Applications Conference*, pages 143–146, 2012.

[32] A. Forget, S. Pearman, J. Thomas, A. Acquisti, N. Christin, L. F. Cranor, S. Egelman, M. Harbach, and R. Telang. Do or do not, there is no try: User engagement may not improve security outcomes. In *Proceedings of the 12th Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 97–111, Denver, CO, 2016. USENIX.

[33] K. Fuglerud and O. Dale. Secure and inclusive authentication with a talking mobile one-time-password client. *IEEE Security & Privacy*, 9(2):27–34, 2011.

[34] V. Garg, L. J. Camp, K. Connelly, and L. Lorenzen-Huber. Risk communication design: Video vs. text. In S. Fischer-Hübner and M. Wright, editors, *Privacy Enhancing Technologies*, pages 279–298, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[35] V. Garg, L. J. Camp, L. Lorenzen-Huber, K. Shankar, and K. Connelly. Privacy concerns in assisted living technologies. *Annals of Telecommunications*, 69(1):75–88, 2014.

[36] V. Garg, L. Lorenzen-Huber, L. J. Camp, and K. Connelly. Risk communication design for older adults. *Gerontechnology*, 11(2):166–173, 2012.

[37] B. Gielen, A. Remacle, and R. Mertens. Patterns of health care use and expenditure during the last 6 months of life in Belgium: Differences between age categories in cancer and non-cancer patients. *Health Policy*, 97(1):53–61, 2010.

[38] S. Gray. Always on: Privacy implications of microphone-enabled devices. Technical report, Future of Privacy Forum, 2016.

[39] P. Gregor, A. F. Newell, and M. Zajicek. Designing for dynamic diversity: Interfaces for older people. In *Proceedings of the 5th International ACM Conference on Assistive Technologies*, pages 151–156. ACM, 2002.

[40] G. A. Grimes, M. G. Hough, E. Mazur, and M. L. Signorella. Older adults' knowledge of internet hazards. *Educational Gerontology*, 36(3):173–192, 2010.

[41] G. A. Grimes, M. G. Hough, and M. L. Signorella. Email end users and spam: Relations of gender and age group to attitudes and actions. *Computers in Human Behavior*, 23(1):318–332, 2007.

[42] R. Gross and A. Acquisti. Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, pages 71–80. ACM, 2005.

[43] M. Haight, A. Quan-Haase, and B. A. Corbett. Revisiting the digital divide in Canada: The impact of demographic factors on access to the Internet, level of online activity, and social networking site usage. *Information, Communication & Society*, 17(4):503–519, 2014.

[44] E. Hargittai and K. Dobransky. Old dogs, new clicks: Digital inequality in skills and uses among older adults. *Canadian Journal of Communication*, 42(2), 2017.

[45] E. Hargittai and E. Litt. New strategies for employment? Internet skills and online privacy practices during people's job search. *IEEE Security & Privacy*, 11(3):38–45, May 2013.

[46] G. Horcher. Woman says her Amazon device recorded private conversation, sent it out to random contact. *KIRO News*, 2018. Accessed on 19 September 2018.

[47] D. Hornung, C. Müller, I. Shklovski, T. Jakobi, and V. Wulf. Navigating relationships and boundaries: Concerns around ICT-uptake for elderly people. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI '17, pages 7057–7069, 2017.

[48] M. G. Hough. Exploring elder consumers interactions with information technology. *Journal of Business & Economics Research (JBER)*, 2(6), 2004.

[49] L. L. Huber, K. Shankar, K. Caine, K. Connelly, L. J. Camp, B. A. Walker, and L. Borrero. How in-home technologies mediate caregiving relationships in later life. *International Journal of Human–Computer Interaction*, 29(7):441–455, 2013.

[50] I. Ion, N. Sachdeva, P. Kumaraguru, and S. Čapkun. Home is safer than the cloud! privacy concerns for consumer cloud storage. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, page 13. ACM, 2011.

[51] Jibo Inc. https://www.jibo.com, 2018. Accessed on 14 September 2018.

[52] S. Jones and S. Fox. Generations online in 2009. Technical report, Pew Internet & American Life Project, Washington, DC, January 2009.

[53] R. Kaye, E. Kokia, V. Shalev, D. Idar, and D. Chinitz. Barriers and success factors in health information technology: A practitioner's perspective. *Journal of Management & Marketing in Healthcare*, 3(2):163–175, 2010.

[54] B. Knowles and V. L. Hanson. Older adults' deployment of 'distrust'. *ACM Transactions on Computer-Human Interaction*, 25(4):21:1–21:25, 2018.

[55] O. Kohanteb, O. Tong, H. Yang, T. Saensuksopa, and S. Kazi. Guidelines for designing connected devices. Technical report, Carnegie Mellon University, 2015. Accessed on 26 February 2018.

[56] S. Kozina, M. Lustrek, and M. Gams. Dynamic signal segmentation for activity recognition. In *Proceedings of International Joint Conference on Artificial Intelligence*, volume 1622, page 1522, 2011.

[57] S. Ledbetter and L. Choi-Allum. Perspectives past, present, and future: Traditional and alternative financial practices of the 45+ community. Technical report, AARP, 2005. Accessed 2 May 2019.

[58] L. Lee, J. H. Lee, S. Egelman, and D. Wagner. Information disclosure concerns in the age of wearable computing. In *Proceedings of the NDSS Workshop on Usable Security (USEC '16)*. Internet Society, 2016.

[59] M. B. Lilly, A. Laporte, and P. C. Coyte. Labor market work and home care's unpaid caregivers: A systematic review of labor force participation rates, predictors of labor market withdrawal, and hours of work. *The Milbank Quarterly*, 85(4):641–690, 2007.

[60] U. Lindenberger, M. Lövdén, M. Schellenbach, S.-C. Li, and A. Krüger. Psychological principles of successful aging technologies: A mini-review. *Gerontology*, 54:59–68, 2008.

[61] D. D. Luxton, R. A. Kayl, and M. C. Mishkind. mHealth data security: The need for HIPAA-compliant standardization. *Telemedicine and e-Health*, 18(4):284–288, 2012.

[62] M. Madden and L. Rainie. Americans' attitudes about privacy, security, and surveillance. Technical report, Pew Research Center, May 2015. Accessed on 30 May 2019.

[63] A. McDonald and L. F. Cranor. Beliefs and behaviors: Internet users' understanding of behavioral advertising. Working paper. Accessed 3 May 2017: http://ssrn.com/abstract=1989092., 2010.

[64] A. McNeill, P. Briggs, J. Pywell, and L. Coventry. Functional privacy concerns of older adults about pervasive health-monitoring systems. In *Proceedings of the 10th International Conference on Pervasive Technologies Related to Assistive Environments*, pages 96–102, 2017.

[65] A. Melander-Wikman, Y. Fältholm, and G. Gard. Safety vs. privacy: Elderly persons' experiences of a mobile safety alarm. *Health & Social Care in the Community*, 16:337–46, 2008.

[66] W. Melicher, D. Kurilova, S. M. Segreti, P. Kalvani, R. Shay, B. Ur, L. Bauer, N. Christin, L. F. Cranor, and M. L. Mazurek. Usability and security of text passwords on mobile devices. In *Proceedings of the 2016 Conference on Human Factors in Computing Systems (CHI)*, pages 527–539, 2016.

[67] S. Mellone, C. Tacconi, L. Schwickert, J. Klenk, C. Becker, and L. Chiari. Smartphone-based solutions for fall detection and prevention: The FARSEEING approach. *Zeitschrift für Gerontologie und Geriatrie*, 45(8):722–727, 2012.

[68] H. Moghimi, J. L. Schaffer, and N. Wickramasinghe. Intelligent home risk-based monitoring solutions enable post acute care surveillance. In *Contemporary Consumer Health Informatics*, pages 399–412. Springer, 2016.

[69] A. Montanari, A. Mashhadi, A. Mathur, and F. Kawsar. Understanding the privacy design space for personal connected objects. In *Proceedings of the 30th International BCS Human Computer Interaction Conference: Fusion! (HCI '16)*, pages 18:1–18:13, Swindon, UK, 2016. BCS Learning & Development Ltd.

[70] J. Nicholson, L. Coventry, and P. Briggs. 'If it's important it will be a headline': Cybersecurity information seeking in older adults. In *Proceedings of the 2019 ACM Conference on Human Factors in Computing Systems (CHI '19)*, pages 349:1–349:11, 2019.

[71] G. Öğütçü, Ö. M. Testik, and O. Chouseinoglou. Analysis of personal information security behavior and awareness. *Computers & Security*, 56:83–93, 2016.

[72] D. Oliveira, H. Rocha, H. Yang, D. Ellis, S. Dommaraju, M. Muradoglu, D. Weir, A. Soliman, T. Lin, and N. Ebner. 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 *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 6412–6424, 2017.

[73] Y. J. Park. Digital literacy and privacy behavior online. *Communication Research*, 40(2):215–236, 2013.

[74] PARO Robots U.S. Inc. http://www.parorobots.com, 2014. Accessed on 14 September 2018.

[75] S. T. Peek, K. G. Luijkx, M. D. Rijnaard, M. E. Nieboer, C. S. van der Voort, S. Aarts, J. van Hoof, H. J. Vrijhoef, and E. J. Wouters. Older adults' reasons for using technology while aging in place. *Gerontology*, 62:226–237, 2016.

[76] S. T. Peek, E. J. Wouters, J. van Hoof, K. G. Luijkx, H. R. Boeije, and H. J. Vrijhoef. Factors influencing acceptance of technology for aging in place: A systematic review. *International Journal of Medical Informatics*, 83(4):235–248, 2014.

[77] Qualcomm Technologies Inc. Home connectivity and integration, 2018. https://www.qualcomm.com/solutions/health-care/home-connectivity-and-integration. Accessed on 14 September 2018.

[78] A. Rao, F. Schaub, and N. Sadeh. What do they know about me? contents and concerns of online behavioral profiles. *arXiv preprint arXiv:1506.01675*, 2015.

[79] B. Reeder, E. Meyer, A. Lazar, S. Chaudhuri, H. Thompson, and G. Demiris. Framing the evidence for health smart homes and home-based consumer health technologies as a public health intervention for independent aging: A systematic review. *International Journal of Medical Informatics*, 82:565–579, 2013.

[80] K. Shankar, L. J. Camp, K. Connelly, and L. Huber.

Aging, privacy, and home-based computing: Developing a design framework. *IEEE Pervasive Computing*, 11(4):46–54, 2012.

[81] D. J. Solove. A taxonomy of privacy. *University of Pennsylvania Law Review*, 154:477, 2005.

[82] D. J. Solove. 'I've got nothing to hide' and other misunderstandings of privacy. *San Diego Law Review*, 44:745, 2007.

[83] StartUP Health. Digital health insights for the 50+ market: Prepared for the AARP. Technical report, AARP, 2014. Accessed 6 February 2019.

[84] E. Stobert and R. Biddle. The password life cycle: User behaviour in managing passwords. In *Proceedings of the 10th Symposium on Usable Privacy and Security (SOUPS 2014)*, pages 243–255, Menlo Park, CA, 2014. USENIX Association.

[85] J. Tao and H. Shuijing. The elderly and the big data: How older adults deal with digital privacy. In *2016 International Conference on Intelligent Transportation, Big Data & Smart City*, pages 285–288. IEEE, 2016.

[86] Theora Care. https://theoracare.com, 2018. Accessed 14 September 2018.

[87] L. Thomas, L. Little, P. Briggs, L. McInnes, E. Jones, and J. Nicholson. Location tracking: Views from the older adult population. *Age and Ageing*, 42(6):758–763, 2013.

[88] S. S. Tirumala, H. Sathu, and V. Naidu. Analysis and prevention of account hijacking based incidents in cloud environment. In *Proceedings of the 2015 International Conference on Information Technology (ICIT)*, pages 124–129. IEEE, 2015.

[89] D. Townsend, F. Knoefel, and R. Goubran. Privacy versus autonomy: A tradeoff model for smart home monitoring technologies. In *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pages 4749–4752. IEEE, 2011.

[90] J. Turow, L. Feldman, and K. Meltzer. Open to exploitation: America's shoppers online and offline. Technical report, Annenberg Public Policy Center of the University of Pennsylvania, June 2005. Accessed on 3 June 2015.

[91] J. Turow, M. Hennessy, and N. Draper. The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation. Technical report, Annenberg Public Policy Center of the University of Pennsylvania, June 2015. Accessed on 24 February 2018.

[92] J. Vines, S. Lindsay, G. W. Pritchard, M. Lie, D. Greathead, P. Olivier, and K. Brittain. Making family care work: Dependence, privacy and remote home monitoring telecare systems. In *Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, UbiComp '13, pages 607–616, 2013.

[93] R. Wash, E. Rader, R. Berman, and Z. Wellmer. Understanding password choices: How frequently entered passwords are re-used across websites. In *Proceedings of the 12th Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 175–188, Denver, CO, 2016. USENIX.

[94] M. Whitty, J. Doodson, S. Creese, and D. Hodges. Individual differences in cyber security behaviors: An examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking*, 18(1):3–7, 2015.

[95] W. Wilkowska and M. Ziefle. Perception of privacy and security for acceptance of e-health technologies: Exploratory analysis for diverse user groups. In *Proceedings of the 2011 5th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth) and Workshops*, pages 593–600. IEEE, 2011.

[96] S. L. Willis, K. W. Schaie, and M. Martin. Cognitive plasticity. In *Handbook of Theories of Aging*, pages 295–322. Springer, 2009.

[97] World Health Organization. World health statistics. Technical report, World Health Organization, 2014. Accessed on 4 September 2017.

[98] X. Yu. Approaches and principles of fall detection for elderly and patient. In *Proceedings of HealthCom 2008: 10th International Conference on e-Health Networking, Applications, and Services*, pages 42–47, 2008.

[99] E.-M. Zeissig, C. Lidynia, L. Vervier, A. Gadeib, and M. Ziefle. Online privacy perceptions of older adults. In *International Conference on Human Aspects of IT for the Aged Population*, pages 181–200. Springer, 2017.

[100] E. Zeng, S. Mare, and F. Roesner. End user security and privacy concerns with smart homes. In *Proceedings of the 13th Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 65–80, Santa Clara, CA, 2017. USENIX.

[101] K. Zickuhr and M. Madden. Older adults and Internet use. Technical report, Pew Internet & American Life Project, June 2012.

A Privacy and Security Risks and Concerns

Table 3: Privacy and security risks and concerns based on Solove's taxonomy [81].

Group of risks	Examples	Supporting quotes
Information collection	Tracking of online browsing.	*"The computer with cookies, they know where I go. They have data about me that I really don't like them having. This whole idea of computers knowing how the users are using the computer and gathering that data and then selling that data to others who make money from that data. I have real difficulty with that,"* P60; *" I know that there are a lot of people are watching what you do on the computer so I don't do anything,"* P5.
	Video and audio monitoring; data collection by wearable and context-aware sensors; surveillance including personal stalking, broader government and political surveillance, and monitoring of older adults by family members, medical care staff, or senior facility management; passive audio and video collection by phones, computers, fall detectors, smart TVs, voice assistants, and home-control systems.	*"We Jews don't face the repression in this country today that we faced in my parent's generation, okay? [...] [But] I am never completely far removed from thoughts of political repression. That's why I talk about surveillance,"* P113; *"These Alexa things [...] I guess it's always on, and always capturing [my data],"* P104; *"A person has some kind of a [...] voice assistant and that [...] record his private conversation and send it to somebody else. So I don't think it is a safe thing to have. I would throw it out of the window,"* P37; *"With the new smart televisions if you know, like with the computer too, they have the camera that they can look at you. [...] Some people cover up the camera with a piece of paper or tape. I am not quite that paranoid,"* P33.
	Violation of bystanders' privacy, especially by voice-activated, video-monitoring, and other context-aware systems.	*"I guess it's like an invasion of privacy. [...] When someone puts you in a room, they should tell you that there's a recorder there,"* P37.
Information processing	Data aggregation; individual profiling; targeted advertising.	*"They know everything you are doing, they know what you are looking at, they know what you are, you know, searching for and everything else. [...] One thing if you are looking at it on the computer, but then if you are talking to somebody and you make a remark about somebody or something or about politicians or something, well somebody could actually gather all that data and use it and say, well this person is a nasty democrat or left-wing or right-wing or whatever, so that is the only thing concerning, about the smart speaker especially,"* P33; *"Everything you buy, everything you look at, even, you know, if I go on Amazon and I look at something, then I'll see an ad for it on Facebook. [...] I don't like all these ads,"* P108.
	Telemarketing, spam (e)mail and calls, and other unsolicited marketing.	*"Oh yeah, you get a lot of weird calls when you are a senior in a rest home,"* P108; *"When you go on to these other sites looking for something then you get a barrage of emails afterwards. And I either delete them and if they keep on coming I try to find the place I can unsubscribe to them,"* P110.
	Fraud and scams (including medical contexts); phishing; identity theft by phone, email, and through social media (including dating websites).	*"They could probably scare me. They could say you have cancer, or you have something that we can't cure, or you need a surgery that you don't need. [...] Just for profit. [...] Let's say that they are a doctor who doesn't accept Medicare or your [insurance] plan, and they say well you have to pay for this out-of-pocket because you think you have cancer and you need a special medication or something,"* P46; *"Somebody was using [my friend's] Kaiser[3] number and getting services at another Kaiser location, and then she started getting these weird co-pay bills and discovered [her medical identity was stolen],"* P71.

Continued on next page

[3] Kaiser Permanente is a major U.S. health care and insurance provider.

Table 3 – continued from previous page

Group of risks	Examples	Supporting quotes
	Unauthorized access to personal information, e.g., by hacking, accidental shared access, or abuse of power.	*"People that shouldn't have access to your records who are in an official capacity could, you know, use information about you that they happen to see. [Say] somebody works at the DMV*[4] *and they looked up address of ex-girlfriend [...] and then they've got out and hurt that person,"* P71.
	Price and service discrimination; jeopardizing benefits older adults might otherwise receive, such as social subsidies, disability allowance, insurance coverage, or eligibility for senior housing.	*"[My personal information] might be used to influence my insurance company to raise my rates,"* P22. *"I am grandfathered in. [...][The director of the senior residence] would like to get us out. She's attempted in the past. [...] We have to [...] report income every year. [...] And when she first saw mine, she was very uppity about why the hell I was there. [...] But if I paid current rent [...], I'd be homeless in 10 years. And she said, 'Well then you would qualify for here,"'* P36.
	Viruses; malware; ransomware.	*"You just can't tell what's a virus and what's authentic. It does make me, I got a virus on my computer from something and got scolded. For falling for something [...] both [by] my son and the repairman,"* P18.
	Data integrity; mistakes and errors in personal records.	*"You wouldn't want somebody putting misinformation in your record. Or [...] changing information in there,"* P71.
Information dissemination	Disclosure; data breaches; selling of personal information to third parties.	*"It's mostly other companies that I never, I really never shopped in the first place that send me emails. [...] Those are the ones that I always want to get rid of. [I: And how do you think they got your information, then?] I'm sure it was shared by others. In fact, I know for sure that the [state] Department of Motor Vehicles sells your name and address. And I don't know what else they sell,"* P110.
Privacy invasion	General concerns about violation of privacy as a fundamental human right; interference in personal decisions.	*"If other people can find out things about you that you don't tell them yourself, yes, I would consider that intrusive,"* P1; *"I have personal knowledge about this type of situation in a family where somebody wants to [...] try to make a case that somebody is incompetent and the only way for them to do that would be, you know, to provide some sort of proof,"*, P47.

Table 4: Consequences of privacy and security violations.

Consequences	Description	Supporting quotes
Financial and material losses	Material and financial losses, including robbery or property damage.	*"Will they get something from my pattern? Would they track my daily activities? [...] So they can break into my house. I'm worried about that,"* P103.
Threats to health or physical security.	Health impairment, injuries, and threats to life or safety.	*I: "How do you think this recorded conversation or medical records or location or activity level or anything can be misused?" "P: Well people can spy on it and then they want to come in and kill you. They want to know when there is no sound and you are asleep, then they come in,"* P37.
Intangible consequences	Emotional, social, or ethical consequences, such as reputation damage, formation of stigma, social judgment, or anxiety.	*"[They could say] 'Oh he has a smart phone and he's [...] going to a meet up place where guys meet up.' [...] It could be interpreted. Surmised [that] I'm [a] bisexual guy. [...] I don't know exactly how they would take it. Or getting rebuffed and stigmatized,"* P9.

[4]The Department of Motor Vehicles (DMV) is a state-level government agency that administers vehicle registration and driver licensing.

B Mitigation and Management Strategies

Table 5: Mitigation and coping strategies.

Passive strategies	Description	Supporting quotes
Limiting or avoiding technology use	Not keeping personally controllable data online or in digital format; not engaging in activities like online banking, online shopping, or social media; not using devices in general.	*"I guess whatever [a computer] knows about me is whatever I have put in or somebody else has. [...] That's why I continue to not use online banking or online payment services,"* P25; *"I don't want [my financial information] on the Microsoft cloud, I don't want it on the Apple Cloud. I want it on a hard drive that I know is on that computer and the portable hard drive that is hooked up. I don't use a wireless backup, a cloud back up,"* P123. *"I am not counting on protection of my privacy. [...] I do not use Facebook, I do not use any social media at all,"* P121.
Using services and devices with good reputations or brand image	Reliance on manufacturers to ensure security protection; confidence that a product with reputable name is safe against security threats.	*"I trust Apple more than most anyone. [...] If you sign into iCloud, if you have that two-layer security turned on, whatever that is called, that's pretty secure stuff,"* P123; *"The nice thing about using Apple, Linux is the system I use, is that there aren't hackers like there are with Windows. Windows everything gets hacked so you have to have an anti-virus, an anti-something-else, and you have to have the firewall. My Mac has two firewalls and that is all I need,"* P25.
Trying to be cautious	Self-censoring transmitted content.	*"I'm aware that there is no privacy, so I would never say anything on my phone or put anything in an email that I felt was in some way exposing me to liability or whatever,"* P121; *"I would do a [Facebook] like [for political figures], or submit [...] and now I've decided not to do that because you just don't know what's being captured. [...] And not like anything bad's going to happen to me, you know what I mean? [Not like] I'll get stopped at the border or something.,"* P104.
	Developing and applying methods to recognize suspicious content or untrustworthy intentions, e.g., in online dating.	*"I try to be very careful with what I get on my email. I don't indiscriminately open every message I get. If it's not a name I recognize, I delete it, I don't even open it,"* P110; *"He's real rich, and he's so handsome. [...] He writes down pages and pages, [...] as far as 'You make my life complete' and he hasn't met me yet! [...] So after a few times, I said, 'You're too good to be true,' and that sets off a red flag,"* P13.
Accepting or ignoring risks	Viewing personal information as an unavoidable trade-off in exchange for safety, or "free" Internet services; avoiding the high financial cost, time and effort, or questionable effectiveness of a remedy.	*"One of the advantages of living in [an assisted living facility] is that they have your complete records, and are in touch with your doctor,"* P121; *"Facebook is free. In exchange [...] you give up all this information because it goes to advertisers. [...] So lots of different things that used to be [...] technically free, they never really were, they were all monetized,"* P71; *"If you give to one pet organization they probably pass your name along to others. You know. I just have come to expect that. That's a part of the electronic age,"* P110; *"Some things you have no control over and can't do anything about. And also some things that you shouldn't be spending your time to do. [...] If you can't fix it or get them to fix it, or don't do anything about that, 'I want my information back' and they say no,"* P107.
Active strategies		
Using or enhancing authentication mechanisms	Using passwords as required; screen-locking PINs; two-step verification; biometric authentication.	*I: "How do you keep track of your password? [...]" P: "I have this file for every company, everything that I use a password, I have it down there. [...] But I try to change them once in a while,"* P13. *"I think if you have the special connect with the hospital or the clinic and you have the special, you have the PINs or the security code, I think it's okay because the other picture over there, you can see which doctor you want to talk to,"* P16.
Configuring settings	Refusing location sharing permissions; deleting cookies; managing audiences.	*"I only have GPS on my phone when I need it. Nobody needs to know where I am—like MoviePass. MoviePass.com apparently wants to know where you are"*, P104, *"I have set [Mozilla] Foxfire [sic] so that when I close [it], all the cookies are deleted,"* P108; *"You can have a universal setting [on Facebook] and then when you post you can change that for the particular post,"* P108.

Continued on next page

Table 5 – continued from previous page

Active strategies	Description	Supporting quotes
Protective software and services	Anti-virus; ad-blocking and anti-tracking programs.	*"Well after being hacked, I don't know if [...] it can really be secure. I mean you purchase this anti-virus stuff that you put on there but it seems like they are not able to do the work. If someone is bent on wanting to get into your data or whatever device. That is pretty freaky,"* P5.
Active management of personal information	Refusing to provide personal information; providing fake information or dummy email addresses; deleting personal records.	*"I never give them my correct personal information. Just email. And a email is just set up for [contests],"* P104; *"As I learn how to use it, I will delete what I didn't feel comfortable with. If it wasn't applicable to me. [...] If it wasn't useful information, I would delete it,"* P60.
Discontinuing services	Unsubscribing, discontinuing, or simply abandoning a problematic service.	*"If you put the freeze [on your account with a credit bureau], nobody can use your name to apply for new credit card. And then if you know something happens, just close the account, right?"*, P103; *"My daughter got me a Facebook account. [...] When she set it up, we went on it together, and I haven't been back,"* P15.

C Troubleshooting: Who Older Adults Turn To

Table 6: Troubleshooting resources used by participants.

Troubleshooting resources	Comments	Quotes
Providers	Older adults in our study most frequently look for help from the service provider, the device manufacturer, or the store/vendor. In some cases, they find these sources satisfactory.	*"The iPad, I went down to Apple, they're always crowded but I went very late and um, I was there for like an hour and a half and they got it—you know, they updated it. So, I think they do a good job because as you say, if you buy equipment and you can't get it to work, it's very frustrating,"* P44.
	However, some expressed reservations about how much time it could take to get help, or irritation at having to deal with chat bots or non-native English speakers.	*"What happens frequently [...] you have a question, an issue, and you're offered live chat. [...] Which really isn't a chat, it's sort of a messaging. I hate it. I cannot, I won't go near it. [...] I want to deal with humans,"* P15.
Personal network	The first call many participants make is to children, relatives, neighbors, or others in their personal network. Some of these helpers are (or were) computer or IT professionals; in other cases, they may only just know more than the participants themselves.	*"I have a guru that lives in southern California. I mail him stuff, we just sent him my computer, the hard drive just died. [This guru] it's my son! He's my computer expert. I want a new computer. I have a new computer. He sends it up, all installed. All I have to do is plug it in,"* P77.
Freelance or volunteer technicians	Several participants also mentioned computer experts they frequently call on—either paid technicians, or volunteers at a senior center or library. Some volunteers are also older adults, who provide help to others in their senior programs or housing facilities.	*"Okay, depending on how bad a technical issue it was, we used to have a guy that, our place provided somebody that used to come to help people with technology. You know, or to teach them how to get around,"* P36.
Do it themselves	Participants may first try to set up the device or solve the problem themselves, either relying on their prior knowledge or searching online for how-to videos, instructions, or help forum postings.	*"I figure them out [the technical issues]. If I don't figure them out, there are one or more persons that I could call,"* P21.
	Less frequently, they may try to find answers in the instruction manual, but some find manuals confusing or opaque.	*"The instructions have to be a, b, c, d, and e. You can't just do a and b and skip c and go to d and e. [...] Smartphones don't always tell you everything that the phone can do. You have to figure it out yourself. I have trouble with that only because it's so complex,"* P35.