Upside and Downside Risk in Online Security for Older Adults with Mild Cognitive Impairment

Helena M. Mentis
Department of Information Systems
Univ. of Maryland Baltimore County
Baltimore, MD
mentis@umbc.edu

Galina Madjaroff
Management of Aging Services
Univ. of Maryland Baltimore County
Baltimore, MD
galina1@umbc.edu

Aaron K. Massey
Department of Information Systems
Univ. of Maryland Baltimore County
Baltimore, MD
akmassey@umbc.edu

ABSTRACT

Older adults are rapidly increasing their use of online services such as banking, social media, and email — services that come with subtle and serious security and privacy risks. Older adults with mild cognitive impairment (MCI) are particularly vulnerable to these risks because MCI can reduce their ability to recognize scams such as email phishing, follow recommended password guidelines, and consider the implications of sharing personal information. Older adults with MCI often cope with their impairments with the help of caregivers, including partners, children, and professional health personnel, when using and managing online services. Yet, this too carries security and privacy risks: sharing personal information with caregivers can create issues of agency, autonomy, and even risk embarrassment and information leakage; caregivers also do not always act in their charges' best interest. Through a series of interviews conducted in the US, we identify a spectrum of safeguarding strategies used and consider them through the lens of 'upside and downside risk' where there are tradeoffs between reduced privacy and maintaining older adults' autonomy and access to online services.

CCS CONCEPTS

• **Human-centered computing** → **Empirical studies in collaborative and social computing**; *Accessibility theory, concepts and paradigms.*

KEYWORDS

Dementia, cybersecurity, scams, risk, discussion

1 INTRODUCTION

Although physical security, such as fall prevention, is regularly discussed within the gerontology literature, addressing safe and secure access to cyber systems, particularly for older adults with mild cognitive impairment (MCI), remains a significant challenge. MCI describes a level of cognitive decline typically associated with aging-related illnesses that requires compensatory strategies and accommodations to help maintain autonomy and perform activities of daily living. This demographic is acutely vulnerable as they are progressively at risk to malicious cybersecurity acts due to their continued functional decline [20]. Yet, when the human-centric aspects of secure cyber systems are considered, significantly limiting or removing one's online access due to cognitive decline is neither practical, nor advisable. For one, continued engagement in the online world offers many benefits, including independence and social and emotional wellbeing [9]. By recognizing that an aging population will continue to want and need engagement with the online world, we necessitate a rethinking of the relationships among security, privacy, and trust in cyberspace for older individuals. The challenge is to design technology that acknowledge the tradeoffs between the practical needs of society and the human values of privacy and autonomy [16]. Strategies in related areas, such as parental disclosure management for parent-child negotiations [2] and post-mortem stewardship of social media profiles [8], may give us a small clue as to the feasibility of new user interaction mechanisms that may allow a once-independent adult to maintain access to their online accounts while also coordinating safe user practices through their caregivers.

Cyber access for those with dementia has been facilitated by the safeguard or surrogate roles family members provide [30]. Caregivers are already going to great lengths to support safe online activity for their care recipients [4, 26, 30]. For instance, caregivers co-manage and assist care recipients in taking care of finances [26] and regularly check the status of care recipients' online bank accounts for suspicious activity [30]. Most interesting is the recent work by Piper et al., that has shown that caregivers for those with dementia may reconfigure social media and email account preferences and settings with more restrictive security options [30]. However, the study gathered the perspective of the caregivers only with little opportunity to uncover how those protections came to be and what was the perception by the person with dementia to the limitations set. This is an important note as cognitive impairment in aging populations is not a static, binary experience. Rather, it is a fluctuating illness of varying stages of impairment with an ill-defined time-frame from years to decades before major neurocognitive impairment may take hold.

The work we present here reveals many complexities that arise from requiring those with MCI and their caregivers to decide on online access in the context of autonomy, risk, and the benefits of interacting online. The success of these decisions hinge on effective shared decision-making to ensure compliance and acceptance of agreed upon security measures. Unfortunately, how to proceed with shared and informed decision making between the parties involved in the evaluation of one's ability to engage in cyberservices is unclear.

In this paper, we uncover some of the evolving needs to enable cyber services access for older adults with mild cognitive impairment. From these findings, we describe user interaction mechanisms that could support the decisions for safe-guarding that access. We assert that new user interaction mechanisms can lead to better shared decision-making, perceived autonomy, and in turn better cyber systems security.

2 RELATED WORK

Aging and Mild Cognitive Impairment

MCI is defined by a noticeable decline in cognitive functioning that goes beyond normal changes seen in aging [23] but has not reached the clinical definition of dementia. It indicates an intermediary stage where cognitive decline becomes noticeable enough to affect daily functioning, yet people can still live independently and have not progressed to dementia. The DSM-V outlines that patients or their caregivers may report symptoms of memory impairment, decline in the ability to perform everyday activities — though patients may still be able to perform these activities without assistance —

and difficulties with language, perceptual-motor and social skills [3].

Mild cognitive impairment commonly presents in individuals also diagnosed with neurodegenerative diseases such as Alzheimer's disease, frontal lobar degeneration, Lewy body disease, and other forms of dementia, or disorders known to impair cognitive functioning, such as Parkinson's disease, Huntington's disease, prion disease, vascular disease, or stroke [11]. Thus, the diagnosis of MCI is prevalent in a large portion of the aging United States population, with recent studies saying as much as 20% of the total US population may have some form of MCI [21]. The prevalence of MCI increases sharply with age, with the most significant rise occurring in patients over the age of 60 [12] — approximately 1-2% of those aged 65 and older, and as much as 30% of those aged 85 and older, have been diagnosed with MCI.

Unfortunately, due to the progressive nature of MCI and its link to aging and other neurodegenerative disorders, symptoms are unlikely to improve. It is important that MCI patients remain in a life-long relationship with healthcare workers and family members to regularly evaluate their abilities and discuss changes in activities to ensure their safety and overall quality of life.

Cyber Safety and Security Concerns of Older Adults

The Consumer Financial Protection Bureau considers financial exploitation of older adults as one of the fastest growing forms of abuse. This is primarily because of the ever evolving form of security challenges online that require education, maintenance and vigilance. For example, older adults who utilize social media are not always cognizant of default privacy settings or how to make administrative changes, as indicated by the small number of older individuals who actually adjust their privacy settings [28]. As a result, older users may accidentally divulge information pertaining to their diagnosis, which may embarrass them and potentially expose them to cyber threats that identify seniors as targets for social engineering or phishing scams. For instance, one of the most prevalent scams is the phone call scam with regards to a "computer problem" or a family member who "needs help". Tech support phone scams result in yearly losses in the tens of millions of dollars, costing each victim an average of $290.90 [25]. Or an older adult unaware of their privacy settings may post sensitive information or geo-location data (e.g., checking in at the bank or hospital) that further exposes them to social engineering threats.

Older adults are also more likely to engage in risky password practices, such as sharing passwords, using the same password over multiple platforms, and using passwords that can be easily guessed [13]. This sometimes leads to the practice of oversight by family members to ensure adherence

to good password practices. Specifically, for married couples, this sharing of information happens because of trust, which places the majority of the responsibility on the partner managing the passwords and secure information. However, having one person responsible for all of the private information in the relationship can also lead to security issues and susceptibility to fraud [33].

Older adults with MCI are even more susceptible and vulnerable online because their continual functional decline puts them progressively at risk of malicious or unintended acts [1]. In general, those with lower levels of cognitive function, lower psychological well-being, and poorer health and financial literacy have been shown to be most susceptible to scams, independent of level of education and income [1]. In addition, if an older adult develops MCI, there becomes a greater need for familial caregivers to be involved in online security due to risks from outside and inside the home. For instance, caregivers must be vigilant of online financial threats that are both adversarial or malicious (e.g., email-based phishing attempts) and accidental (e.g., overspending on unwanted or repeat items online). Piper et al. [29] found that there are even new and specific adverse financial threats for people with MCI such as online offers in emails that led to exorbitant purchases and phishing attempts due to one's medical condition leading to the purchase of a 'cure'. This required the caregivers to employ spam filters, set restrictive privacy settings, and block inappropriate content (e.g., adult websites) in order to protect their loved one.

Person-Centered Design for Older Adults

The problematization of aging is a fairly prominent viewpoint in the HCI literature [37] [32]. Vines et al. [37] showed how this declinist view dominates much of the studies of older adults and, in turn also dominates the body of knowledge that researchers and developers draw upon in their framing of technology support. It is understandable that in devising technological solutions, focusing on one's physical and functional limitations provide actionable challenges and a mechanism to show measurable results [24]. However, Vines et al. [37] also highlighted how a turn away from a problem-focused model allows for the individual to define for themselves what successful aging is and how that may provide the needed sense of worth in the face of any illness or challenges.

More recently, Lazar et al. [19] and Madjaroff et al. [22] both argued for a turn away from a medical model of designing for those with dementia and instead engage in various person-centered models. Lazar et al. [19] put forth a critical dementia perspective that recognized people with cognitive impairment as making meaning in a contextualized and social manner, engaging in similar physical and embodied interactions that display meaning, responding to and participating in the world through sensory experiences, and continuing to engage in emotion and affective experience. Likewise, Madjaroff et al. [22] argued that the design of technology for those with dementia are disability and change focused and in turn shape the identity of the very people they are to help — reifying their dependency and their loss of self. role of technology to provide support within the dyads' life. They uncovered the desire of technology to support biopsychosocial aspects of autonomy for both the caregiver and care receiver.

Thus, in the following work, we are motivated to find a solution to continued secure online access for older adults with MCI that is person-centered [17] [18]. For one, we will not immediately start from the perspective that old age and MCI is causing a 'problem' that needs to be 'fixed'. Second, that there is no one right approach to be taken when faced with the conflation of autonomy and security. And third, to create mechanisms for a person with MCI to feel they have a say in the approaches that are put into place.

Downside and Upside Risk

In order to abide by a person-centered approach and better understand the tradeoffs in ensuring an older adult with MCI can still engage in online activities while remaining secure, we turn to the gerontology literature on physical safety and risk. Focus has been given to the physical safety of older adults — for example fall risk has been closely examined both in practice and in research. Within that context, the concepts of downside and upside risk have emerged in describing how to balance the need for safety while still maintaining a semblance of autonomy.

When an elder has a fall, they are considered to be unsafe and are usually wheelchair bound after such an incident. Although done with well-meaning intentions, the elder is disempowered in being physically active, which over time does more harm than good. This is called downside risk. Downside risk describes the probability of an outcome that is worse than the benchmark — the benchmark in this example would be falling and breaking a hip. On the contrary, upside risk describes the probability of an outcome that is better than the benchmark. Being able to regain physical strength by walking and moving around even after an accident may be valuable enough to justify taking the risk of possibly another fall.

The bias in the aging field has historically been toward accepting downside risk regardless of how much we diminish the possibility of a better than expected outcome. The recent movement of person-centered care in aging services has instantiated a different care model that tries to balance safety and security with the older adult's need for autonomy.

A great deal of research has confirmed the functional impact of experiencing autonomy as opposed to heteronomy in important life decisions. Undermining autonomy typically detracts from intrinsic motivation, creativity, self-motivation, confidence, interest, and vitality [10, 31]. Studies in nursing homes have reported that residents who were encouraged to engage in decision-making were more alert, active, and happy than were residents who were treated in an infantilizing manner, even if it was for their safety and in their best interest [30].

We can see this tension in the research around human-centered cybersecurity as well — particularly between the tradeoffs in security and privacy [16]. In addressing cybersecurity issues for older adults, minimizing downside risk and promoting safety for older adults in online interactions is clearly important, but understanding and considering the upside risk of an older adult with MCI seeking to engage online as long as possible may be more important.

3 METHODS

Our aim in this work is to first determine how a person with MCI and their caregiver are addressing cybersecurity incidents and concerns, if at all. We then aimed to determine if the approaches taken are engaging in downside or upside risk. From there, we further articulate what forms of support and intervention might be beneficial from a person-centered approach.

Study Design

We began with a set of interviews of older adults with MCI and their spousal caregivers to identify current cyber system access practices and anticipated needs.

In interactions with our user population, we employed a person-centered approach to the interview process. The person-centered approach emphasizes the following strategies that are easily employed in studies with users who have dementia [38]: (1) Engage with the person in a comfortable and familiar environment (e.g., interviews or participation should be in a familiar space rather than convenience); (2) Consider the elder's schedule and the culture of their residence (e.g., interviews should not be held before or during lunch time); (3) Focus on regularity of people and events to optimize memory and reduce fear of failure (e.g., care partners should be involved in the process). Our experience has shown that a participant with MCI may not be able to engage in a long, cognitively demanding interview session. Because of this, we kept each interview session to one hour and performed a second interview if further questions were needed.

In addition, we aimed to interview our couples as a unit as the sense of identity of the person with cognitive impairment is a product of the dyadic caregiver-care recipient relationship. Mulvenna et al. [27] and Whitlach et al. [39] also argue that this approach actually enhances the inclusion of the care recipient's thoughts and experiences rather than diminish the care recipient from interacting. This is because if you compromise the person-environment fit, which includes their caregiver as a main actor, you are less likely to have a rich discussion. In our case we had no evidence of the caregivers dominating the conversation — in fact, when the care recipient was at a loss for words, they would look to their caregiver as a guide to fill in the gap. This approach to technology studies and dementia leads to a more user-centered method that focuses on the individuals suffering from the disease and uncovering both their experiences as well as the experiences of those caring for them.

Participants

The first phase of our study included participants from the Integrace Institute, which helps families and patients deal with a dementia diagnosis. The participants were part of the Institute's outpatient clinic and do not live on the premises as residents, but rather at home with a family member. Participants were recruited with the help of the Institute's Director of Research. The inclusion criteria were a diagnosis of mild cognitive impairment by an on-staff neurologist at the clinic. In total, six couples were interviewed. The sample size was constrained due to (1) the narrow inclusion criteria of a diagnosis of MCI (2) saturation was quickly reached by six dyads. Applicable demographics are presented in Table 1. Although we did have a variety of background, overall, our participants are middle-class and so some of our findings will be idiographic.

Procedure

A flyer was distributed to all of the applicable clinic patients directing them to call the Dementia Research and Education Associate at the Integrace Institute if they were interested in participating in the study. Those who indicated an interest in being involved would then schedule a visit with the second author of this paper through telephone or email. The interviews occurred on the Institute's premises (D1, D2) in a private conference room or in the participant's homes (D3, D4, D5), if they preferred. Participants had to have the ability to provide informed written or verbal consent to being involved in the research.

A strong ethical framework was essential in guiding our research [23], particularly because we were working with a vulnerable population. This framework focuses on several aspects: respect of the individual with impairment and their caregiver (not looking at our participants through the medical model lens, or as disabled or sick); making sure the opportunities for research participation are available in the

Table 1: Care Receiver and Caregiver Demographics

Dyad ID	CR gender (age)	CG relationship (age)	MCI Dx	CG Employment status	CR Previous employment	Socio-economic background
D1	Male (74)	Wife (72)	18 mo.	retired	scientist	upper/middle
D2	Male (78)	Wife (76)	6 mo.	retired	teacher	upper/middle
D3	Female (64)	Husband (65)	12 mo.	employed	horse rancher	middle
D4	Female (76)	Husband (77)	24 mo.	self-employed	nurse	middle
D5	Female (72)	Husband (72)	16 mo.	retired	worked for NIH	upper/middle
D6	Male (74)	Wife (70)	3 mo.	retired	IT	upper/middle

least intrusive and restrictive way [23] and assuring that all confidentiality protocols have been followed closely, including gathering and storing our data. We have firmly complied with our IRB's requirements to "do no harm" to those who are considered vulnerable, particularly cognitively impaired older adults [23]. Diagnosis of a dementing illness does not presume incompetence and that is why all MCI participants had to be able to provide their own consent. But, we also asked that the person's caregiver or "surrogate" [15] provide consent for them; in all of our cases, the surrogate consent was provided by the spousal partner. Upon completion of the IRB requirements we proceeded with our interview.

Semi-structured interviews were employed. The interviews began by getting to know both the individual with MCI and their care partner by asking them to tell us the story of how they met. We asked them to share any family and health history they felt comfortable with, including their experience with the diagnosis of cognitive impairment. On more than one occasion however, we would hear about love stories, grandchildren, and be shown Bat Mitzvah home videos. All of the participants in this study were kind enough to share details about their daily life, daily care and how they were coping every day. We then asked open-ended interview questions around online access and cybersecurity: (1) what cyber security and safety issues have already occurred, (2) whether they have instilled any safeguarding practices to date, (3) what concerns they have regarding online activity for the future, (4) whether they have thought about how they would modify their use of online cyber services and (5) if they had ever considered who would be the responsible party to manage that access as the MCI progressed.

Data Collection

Interviews were video and audio recorded and later transcribed for detailed content analysis. Since we were asking participants what online interactions they enjoyed using, they sometimes showed us their smart phone or other device so video recording was essential to capture these demonstrations. We were also interested in catching those nonverbal

moments of interaction that better conveyed the dynamics of the couple. In particular, anything that might have conveyed that the answers being given were either coerced or untrue — from the video, we were able to be confident in the validity of the experiences our participants shared. Finally, the video recordings allowed us to revisit important elements of these conversations and pick up on cues, particularly from the person with MCI, ensuring validity [10]. By using a semi-structured interview method, we were able to elicit deep and meaningful narratives about the family's lives. The primary advantage of conducting interviews in a health-related problem space is to allow the researcher to focus on the participants' perceptions and ultimately inform about their experiences and those of their caregivers [10]. As we explore a user centered approach to security, it becomes increasingly important to look at the domestic context of an individual and shared activities in the household, particularly with the growth of online activities [34]. This perspective is also important in how we chose to conduct our interviews — involving both partners in the caregiver/care-recipient marital relationship in a real-world environment.

Data Analysis

Thematic analysis was chosen to systematically analyze the data [6]. This provided us with the ability to move beyond surface level similarities to more tacit themes. The analysis focused on how the couples spoke of their online experiences and their perspective on online access now and in the future. Subsequent integration of these themes with our interpretation of the literature, security, and risk helped us form the basis for the discussion of design implications. The analysis was primarily conducted by the first and second author - the first author would first code the data and then discuss the themes and examples with the second author. The third author was then later engaged in the interpretation of the themes and examples.

After an initial thematic coding of the data, three primary themes arose: experiences with technology, safeguarding approaches, and cybersecurity discussion. Further analysis

and delved into these three themes. The first was a focus on how the dyads spoke of their technology experience. We uncovered themes around the prevalence of technology in their lives, their comfortableness with technology, their awareness of cybersecurity concerns, and security incidents that have occurred. The second focus of coding the transcripts focused on the types of safeguarding approaches the dyads have taken. This is where the different categories of approaches we will talk about arose. Later, as we were aligning our findings with prior work, we went back and coded each approach as either upside or downside risk - the second author was the expert in this regard. The third part of the coding was the way in which planning and discussions around cybersecurity in the future were manifest. All quotes are evidence of the existence of these main themes, but are not the only examples we had in our data.

4 FINDINGS

High Digital Literacy & Security Knowledge

We uncovered that our MCI participants were engaging with a number of web applications and some would even say they were very comfortable with using technology and the Internet. For instance, one of our dyads was a relatively "newlywed" couple that met on the Internet.

> C3: It'll be 10 years May the 13th. Exactly. Guess where we met. Match.com.
> P3: Absolutely.
> C3: Technology all the way.
> P3: That's right. I would have never found him any other way. He's all Mr. Techie.

All of our participants have clearly integrated online engagement into their daily lives through the use of gaming, video-calling family members with applications like Skype, keeping in touch with grandchildren via Facebook, purchasing products online, and viewing their online banking statements. For instance, the following MCI participant was discussing her comfortableness with buying products online, including shoes.

> P5: One time I needed shoes for something, and I ordered like five pairs of shoes and then I had to send them all back, it was very annoying because I spent more on the cost of shipping for the shoes because I didn't . . . what is it . . . Zappos . . . So I had to pay for them to come and I had to pay for them to go. Yeah I do use [my credit card] for shopping occasionally and things like that.

Even for those participants whose MCI was causing significant issues in engaging in activities they once found enjoyable, such as reading books or knitting, our MCI participants were finding ways to still engage and communicate with their Internet-enabled devices. For instance, in the following example, P4 has experienced significant reduction in what she can do due to her MCI, yet she has found games she can download from the Internet and Facebook to still be a part of her life.

> C4: The Kindle she found Solitaire. She found ... I think I put a Dominoes game ... for you. You were playing Dominoes.
> P4: That's fun. Yeah.
> C4: You try to get different games.
> P4: I know there's more [online apps I use]. I have a Facebook page.
> I: Oh, you do?
> P4: Yeah. I like to see my grandchildren grow up.

And in the following example, P3 also plays games and uses Facebook to connect with her family even if she does not remember the interactions.

> I: Are you ever interested in posting on Facebook or do you look at kids' pictures or the family photos?
> C3: She does. She forgets it.
> P3: I do on occasion. My biggest thing is the game. What's my game, honey?
> C3: Solitaire.
> P3: Solitaire, yeah. I do that, but then- it just depends. Sometimes I go on the Internet, but I'm not a geek like he is.
> C3: She has the same phone that I do. She can log on to that phone. She doesn't know she's on Facebook, but she is. She always looks at pictures. Like [family member name]. [Turns to wife] How many times a day do you see [family member name] post and you always talk about her and ... [Turns to interviewer] She still does that. My cousin in Tennessee does a monthly luncheon so there are about 30 cousins and family members that get together once a month to eat and she saw that and she said, "Hey, we miss you guys. We wish we were closer." She's always commenting. She does a lot of stuff like that without remembering the details of it.

Thus, our participants are already invested in their online access — it provides entertainment and socialization as well as a tool for convenience — in other words, this is not a population that can be described as technologically adverse or naive. They gain the same benefits from online access as any younger generation or less impaired cohort does.

In addition, we cannot describe this population as technologically illiterate — or more to the point security illiterate. The dyads that participated in our study all had a fairly informed understanding of the potential pitfalls of owning an Internet-enabled device and sharing personal information through the Internet or on the Web. For instance, they might have one credit card they use for online purchases (D5), they do not enter sensitive information online (D2), they get

antivirus software on their PC (D3), and they consider the tradeoff of the security of an iPad versus a PC (D4).

For instance, the following participant who has MCI regularly makes purchases online and thus has one credit card for just that purpose.

P5: I have one credit card that I keep for mainly online purchase like Amazon. I'll purchase stuff or-
I: And so you feel safer using one specific credit card because you can monitor and kind of make sure-
P5: I don't really feel safer, I just feel better.

So, this person is still aware of the potential dangers and has a plan to mitigate her risk. Yet, she understands that there is still a potential risk out there. This shows a nuanced understanding of Internet security that is fairly above average.

Experience of Minor Security Incidents

The families all shared at least one recent incident that brought to light safety and security concerns with online interactions. Most of these were relatively minor in terms of the outcome: i.e., there was no money lost or computer data compromised. They included a spoofed email (D5), buying a scam product online (D3), or reacting to or sharing something on Facebook that is out of character (D4, D6).

Some of these incidents are understandably observed by the caregiver and are a source of concern for them. For instance, C3 is concerned with the constant barrage of scam cures that his wife may purchase without his knowledge

C3: Every now and then, [my wife] will get on the internet and she'll find somebody who's selling some magic cure and she'll start playing that. I'll tell her, "I've already heard that one. We've already bought that one. We don't use that one and it's a ripoff, so don't listen to it, because we're not buying it again." Because she went on one time and ordered some stuff ...

Some minor incidents could lead to significant embarrassment, though, if they are publicly made. For instance, a number of our participants had mistakes on Facebook that were embarrassing and caused family tension. For instance, C6 related the dramas she has had with her husband's use of the Facebook like and share features.

C6: My youngest sister, I have a sister that's 56, she said, "if he likes Jesus one more time, I'm gonna beat the crap out of him." ... The other day ... I said, "Did you read this that you liked, or made a comment on?" [imitating husband] "Well no, I just kind of liked that." [own voice] I said, "Would you please go a little deeper and read. Because this is garbage. And I know you don't think that way."
P6: If it's too long to, I don't read it.

C6: If you click on "Impeach Nancy Pelosi" one more time! She's not your Congresswoman! She's from California. You know what I mean? What are you doing?

Here it is clear that, although a minor mistake, the person with MCI is beginning to have difficulty reading longer articles, as well as critically think about what to react to and share on social media. It is interesting that the caregiver notes that his recent likes and shares are not reflective of what he thought — at least before the MCI — and so are a minor indication that further intervention may be needed.

On the other hand, our MCI participants also were aware of when a decline in their cognitive abilities was beginning to manifest in online interaction. For instance, P5 was well aware of the risk of scams and misleading emails and, yet, because of the following incident, does not feel she can discern a fake email anymore.

P5: Like I said with that Yahoo thing, I finally took it into Staples because I had answered it and everything, and I love Staples, they'll talk to you about anything. The old guy just looked at the email and he said, "Oh no, this is not a real email." But it looked so real to me.

And P4 made a mistake on Facebook and now she has her husband, C4, interact with the application on her behalf.

C4: She used to actually she'd do everything, do some typing into it [Facebook]. ... One time she hit a button by mistake. Our son said, "Why did you dislike what so-and-so said?" [Wife's name] said "I didn't dislike it." "Well you hit the no button" or something. Even I was confused once by it, because I think the default had already pressed yes. I guess she thought she was pressing yes, instead it was no. I probably would've done that myself.

The 'adverse event', as coined by Piper et al. [30], might not be a significant breach of security, but rather a small incident that in and of itself might not be a huge concern. Only in juxtaposition to prior behavior and the contextualization of the potential for further risky behaviors in the future, the event gives rise to a realization by the person with MCI and their caregiver that there needs to be a solution put into place. And we can see that a population who is still fairly autonomous and aware of their behavior, can contribute to an assessment of that potential for further risky behavior.

The Spectrum of Safeguarding Approaches

Once we had a better understanding of our participants and their experiences with cybersecurity incidents to date, our next line of questioning evaluated what steps our dyads had taken in response to these incidents, if any at all. Four of our six participants articulated steps they have taken to address the concerns of continued online access for the person with MCI. In the following findings, we describe the approaches taken as well as describe the care model taken in terms of

upside or downside risk. Assessing upside and downside risk has to take in many facets of the situation — for instance, how significant is the illness, how often has there been an incident, as well as what are the wishes of the person with MCI. Our assessment of upside and downside risk is due to the overall assessment of the approach and we concede that for the particular couple, an approach we deem a downside risk, may be an upside risk for them.

Solutions to adverse events varied widely and seemed to have no relation to the months since the diagnosis of MCI. It is interesting to note that no one had taken the steps of completely removing all online access. However, for some of the spousal caregivers we interviewed, they have begun to limit autonomy and by extension the potential unsafe interactions their spouse can have on the Internet. This limitation could be quite significant in limiting all unsupervised interactions. For example, C3 had a succinct way of addressing security threats:

C3: Being right beside each other all the time. I know what she's doing and she knows …

In terms of upside and downside risk, this approach — the 'Hover' — is downside risk as it leads to a loss of privacy and autonomy for the care recipient and seems to place all decision-making in the hands of the caregiver. There still is the positive value of continued interaction online, but the cost may be seen as too much with regards to autonomy and privacy.

Limiting access for the care recipient was also used by this caregiver (C3) to help their wife who has MCI to continue with her chosen activities.

C3: If you go look at her desktop … [Turns to wife], can you minimize the solitaire and show her what your desktop looks like? [Turns back to interviewer] So she has two icons, right? She could go find [something else], but it doesn't interest her. Whatever she wants to use is right there on the bottom, so if you look at the bottom, what's there? Internet Explorer, solitaire …

We also deem this approach — the 'Selective Access' — as downside risk, but a lesser form than the "Hover". This is due to the person with MCI having some semblance of autonomy and decision-making ability as to what, of the limited choices, they would like to do. It is important to note as well that a caregiver can take multiple approaches, as we see here with C3 — although both of these approaches are downside risk.

In other instances, we have a caregiver who is becoming the interactor on behalf of the person with MCI who may not be able to interact with the system themselves anymore. For example, the incident explained prior regarding an odd Facebook post led to mediation by C4.

C4: At one point, [wife's name] was looking at her Email, but then she asked me to check the computer now for an Email or Facebook. Now, what I'll do is I'll go on the Facebook page for our granddaughter and so we can see our great-grandchildren. If I get an Email that there's something, somebody is posting something, I'll let [her] know and I'll go to the page so she can see it.

In this case we are seeing an approach — the 'Interactor' — as a borderline case of upside risk. It could be downside risk if the person with MCI was not involved in the decision to engage in an approach that removes autonomy and privacy. However, in this case, this person with MCI was our longest diagnosed case and was beginning to have significant cognitive issues. Due to this, as can be seen in the quote, the wife asked the husband to engage in online interactions on her behalf. And so, as the person with MCI was engaged in the decision making and the steps taken were done in the hopes to still retain value from online interactions, we deem this upside risk.

We also had two approaches that were on the lightweight side of the spectrum. And as can be seen in the following examples, some participants with MCI continue to engage with online applications and websites with a minimal 'check' on their activities by their spousal caregiver or offset the work to tools like automatic bill payments or saved passwords.

P1: Yeah, you know I used to do all the travel arrangements. I used to handle a lot. Now my wife has to take on a lot more. I would book our travel and I still do, but now I go through all the steps on Orbitz and then I ask her to check everything and she finalizes and pays for it.

P1: Sure I can do online banking. I can set up most of these things, unless the password doesn't work or something or that kind of stuff … but [my wife's] taken on a lot of that for me.
I: So, she's taking on the responsibility?
P1: The responsibility to check. Most things, you know, I pay bills … just automatically, you know.

C6: He has no idea what his passwords are because he doesn't use them. Because it's on his phone, he goes right in but they are in your contacts under that.

In the first and second quotes, P1 is explaining how his wife is now a second pair of eyes on everything he is doing. This upside risk approach — the 'Checker' — was the decision of the person with MCI, but more importantly allows the person with MCI to continue to be fairly autonomous and retain some semblance of privacy. And then in the second and third quotes, P1 and C6 are providing an example of an upside risk approach — "Automation" — that using the computer itself to provide some security by removing the likelihood of a mistake by the person with MCI.

Finally, our two participant dyads who had not taken any steps, D2 and D5, have, without probably realizing it, engaged in the upside risk approach of 'None'. They have chosen to not take any oversight or preventative measures yet and have weighed benefit of online interaction against the risk of another incident.

What we have thus found is a spectrum from complete oversight to mediation on behalf of the person with MCI to a light check or nothing at all. This highlights the complexity of finding the right balance between continual online interaction and safe and secure online access.

When and How to Discuss Cybersecurity Concerns

There was a lack of discussion, forethought, and planning for progressive cognitive decline. This lack of planning took two forms. The first category of planning is to determine what online interactions need to be transferred to or overseen by the caregiver. Only one MCI participant had begun to hand over certain responsibilities to his wife because he knew it needed to be done.

> P1: [My wife] still has difficulty doing it, but she's taken on a lot of that [online banking] for me.

The second category of planning is to ensure that all passwords and online access is at least saved somewhere for use by the caregiver when needed. The following caregiver was, at this point, the holder of all of the passwords. But she also went a step further by setting up backup password holders.

> C6: I have a sheet typed up with our passwords and how to get into our banking, et cetera. My sister said to me, "If something should happen to you, you go into a coma or something, he's no good in an emergency. Where's your stuff written down because he won't know." And you're right, [to husband] you wouldn't know. So she said, "Email it to me and to your kids." And I also took pictures of where the stuff was and sent it out.

The rest of our participant dyads were just reacting to incidents and had no long-term plan with regards to passwords and how Internet access might be monitored or curtailed as the cognitive decline progressed. What is surprising is how, overall, our participants had been so on top of everything else with regards to their financial and health decisions. They all had a lawyer, a will, power of attorney, and advance directives. But it never occurred to them who should be held to account for online access and behaviors and then how to go about monitoring and/or controlling that access.

One concern that is brought to the fore when considering how one's online access should be monitored or shaped is who is the person that should be entrusted with this oversight. Not every spousal caregiver is comfortable themselves with online interactions.

> P1: My wife was never interested in doing this. She still has difficulty doing it ... So, I've tried to get her [wife caregiver] more involved with all these technologies over time. She's done fairly well in doing that. So, I'm relying on the fact, as my dementia problems increase, is that she would be there to do that for me. Maybe that isn't the best approach and my fall back is for one of my grandkids to do it. I would love to give it to my daughter, but I'm always afraid that she's got so many things on her plate too.
> I: You just sort of don't want to bother her?
> P1: Bother her with all that kind of stuff.

Thus, just as participants worry about who should have power of attorney or advance directive over them as they age, once confronted with who should have power over their digital lives, the same concerns of burdening a loved one manifest. And similar to all discussions around planning for aging, health decline, and death, our participants shared their concerns that there is never a good time to talk about it with loved ones.

> P1: It's a good idea to actually share that with some of your family members. If you've never been really close to some family members when you gotten things going on and you sit them down and say, "We're going to stop and we're going to have this family conversation about A and B." Or they'll say, "Why are you doing this? Dad, you, mom, because we're fine, you're fine."

This exposes a real need to guide these conversations as well as provide options for what and how to support their loved one's continual online engagement through their cognitive fluctuations.

5 DISCUSSION

Through our interviews, we have first determined a spectrum of approaches taken that includes both upside and downside risk. Downside risk is the result of taking steps to ensure safety, but ultimately causing harm in the process — such as when confining someone to a wheelchair to prevent them from falling can lead to further health complications and reduced mobility. For our uses, this would be equivalent to taking away all online access for a person with MCI to prevent their exposure to potential scams or security breaches. The harmful result of that course of action may be the isolation and resulting depression and further, and perhaps faster, cognitive decline of the person with MCI. Thus, an increase in safety comes at the cost of autonomy as well as the addition of further health problems. Upside risk, on the other hand, is taking a course of action that assumes some risk, or loss of safety, may occur, but the outcome, if successful, is much more ideal. For instance, rehabilitation therapy for strength and balance may not remove all risk for falling, but

the potential for less falls and increased mobility that enhances one's autonomy may be worth the tradeoff. Likewise, for our cybersecurity concern, supporting a person with MCI to continue to engage in the online world, but encouraging that engagement with safeguards in place.

We see this approach for upside risk with many of our families. Either playing the mediator role or being a second set of eyes can be used as a mechanism by which family caregivers are trying to maintain their care recipient's autonomy while ensuring there is a modicum of safety. Likewise, the spectrum of safeguarding approaches taken is highlighting that there is no upside versus downside, but a spectrum from fully upside to fully downside taken.

However, what we are not seeing is an understanding of the trade-offs being taken in choosing a strategy, a plan ahead for how to address the inevitable decline, and any form of regular proactive assessment of abilities and desires. All of our participants agreed that ensuring they are prepared for the future in terms of their digital life is a great idea, but they remain keenly aware of the lack of support in making these decisions. Most participants agreed that unless there was an adverse event that occurred which forced them to take any serious action, they would not be prepared or well equipped to safeguard their digital lives in the future.

So, how can we design user interactions that support continual safe online interaction that is responsive to the changing needs of the older adult with MCI?

Mechanisms for Discussing and Setting Access and Control

Recent work on how parents manage their children's identities online has suggested solutions such as shared online accounts that allow cooperative content management for children to negotiate their online identities with their parents as they transition into adulthood [2]. Similar features had been suggested for those with dementia such as a shared account [30]. In contrast to the transitions experienced by children and parents, a person with MCI was, at one time, fully autonomous and now requires fluctuating levels and forms of support. For this reason, it is tricky to balance the need for security, while also considering how to allow autonomy and individuality to remain in a cooperatively negotiated experience that empowers care recipients. Notably, problems can arise when there is one single shared account. For instance, caregivers vary in whether they seek approval for performing online actions on behalf of their care recipient [30] and when an individual is responsible for another person's information disclosure, errors in judgment and even deception may occur [29].

We look to the relatively recent introduction of legacy contacts in the social networking site, Facebook, in order to navigate the ethical and legal challenges that sharing an
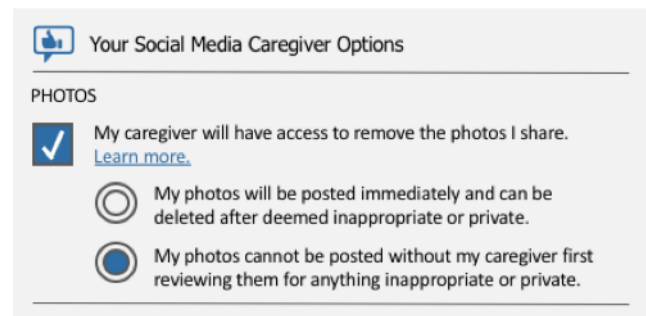
Figure 1: Example of One Possible Setting for Social Media with Downside Risk and Upside Risk Options
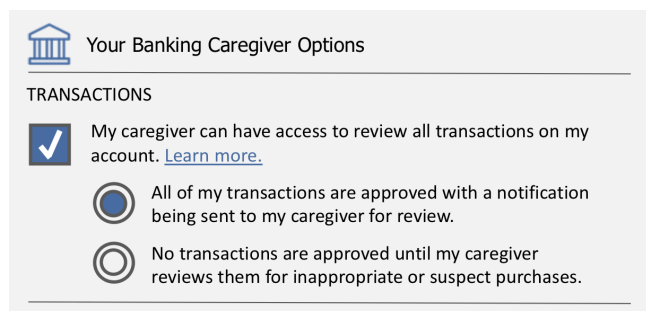
Figure 2: Example of One Possible Setting for Online Banking with Upside Risk and Downside Risk Options

account might present [4]. In response to the challenges of how to handle one's profile when deceased [7, 8], a person can now designate a legacy contact to maintain control over the deceased's profile along with the option for some further access to one's personal information. A mechanism such as this provides us with two useful design decisions: a mechanism to support proactive discussions and a mechanism to allow for tiered access to one's account.

Proactive mechanisms that support discussion between care recipients and caregivers could be beneficial. Discussions regarding access and control or management of downside and upside risk for cyber-services may reduce the prevalence of adverse incidents and increase the care recipient's autonomy. Crucially, organizations supporting shared decision-making towards a plan that values cyber-security would also benefit by fielding fewer security and privacy support concerns from caregivers.

For example, a shared decision-making interaction mechanism could present the option of a caregiver to have the ability to delete the care recipient's social media posts if deemed inappropriate (See an example of one possible setting option in Figure 1). The downside risk might be that no such posts will be made again, ensuring that all posts are appropriate according to the caregiver. The upside risk

might be that even if a post is deemed inappropriate by a caregiver, they should first consult with the care recipient before having the authority to delete, even if the posts stays live for a period of time. The older adult with MCI still has the autonomy to make a decision, there is simply a more open conversation about upside and downside risk to their behavior.

Another example would be if the caregiver should have the ability to review all credit card transactions as soon as they are made and put a stop to a malicious financial attack (see an example of one possible setting option in Figure 2). The downside risk might be that the caregiver takes full control of the care recipient's bank account so any malicious acts can be prevented immediately. The upside risk might be that the care recipient continues to have control over their bank information with the caregiver's ability to review credit card transactions.

In both of these examples, we have only provided two options; however, from our study, it is clear that the spectrum of approaches means there are potentially many more options for both downside and upside risk.

The Feasibility of a Spectrum of Risk Options

Notably, digital asset co-management is an important issue beyond end-of-life planning, and new laws are vague as to family members' legal right to share passwords [40]. Addressing this need for cooperatively negotiated access beyond the one-time event of one's death is a challenge that will continue to arise as our population continues to age.

The challenge here is twofold. First, the Computer Fraud and Abuse Act (CFAA) treats a shared password as an unauthorized access. In security, authorization is the process of determining who should be allowed to use a service. This is different from authentication, which is the process of presenting and verifying an identity credential, typically a username and password. Thus, a shared password is, from a legal standpoint, indistinguishable from any other unauthorized access. Technology policy organizations like the Electronic Frontier Foundation (EFF) and Center for Democracy & Technology (CDT) would like to update the CFAA to address this concern. They believe a voluntarily shared password is fundamentally different from someone hacking into an account without the account owner's authorization.

Second, much of this legal rationale relies on terms of service or terms of use documents that typically require the user of an online service to "agree" not to share credentials with anyone else. If this behavior is the norm, then viewing any shared passwords as unauthorized access is fair. However, companies could change their terms of use to enable MCI users to share passwords with a caregiver or even create separate authorized caregiver accounts similar to the legacy accounts Facebook uses. If companies did do this, then the

legal concerns about unauthorized access would disappear without the need to change or update the law.

Privacy by Design

Although the security community has understood for some time that systems must be secure by design, the privacy community is only realizing these lessons apply to their domain as well [14]. Proactive mechanisms supporting either transition or negotiation of access control must be deeply and carefully integrated throughout systems seeking to support caregivers and care recipients. Features like Facebook's legacy contacts require architectural changes which are known to be difficult to "add on" later [14, 36]. The traditional approach to privacy (i.e., a regulatory- or policy-oriented approach) is failing [14], and we must treat privacy as a first-class concern throughout our engineering process [35, 36] to address this failure.

Deeply understanding how engineering decisions affect the privacy of real users is not easy. Facebook's recent "emotion contagion" study demonstrates the disconnect [5]. The sort of A/B testing used when Facebook altered news feeds for over 680,000 people to see whether exposure to emotional content would affect how users posted is common practice in industry, but it remains unknown to most users, many of whom were outraged when they learned of this practice [5]. Privacy and security must be considered holistically and throughout the design of software systems for the proactive mechanisms suggested herein to be successful.

6 CONCLUSION

With the growing aging population, we cannot overlook the importance of establishing cyber systems that are reliably integrated and effectively used by older adults who have cognitive impairment. That is the central thrust of the research here; its broader impact lies in providing the impetus to explore systems that help negotiate and support secure and trustworthy computing without hindering a person's activities, autonomy, and choice.

REFERENCES

[1] Linda M. Alves and Steve R. Wilson. 2008. Depression and Elder Abuse and Neglect among a Community-Dwelling Chinese Elderly Population. *Journal of Elder Abuse & Neglect* 20, 1 (2008), 63–85. https://doi.org/10.1300/J084v20n01

[2] Tawfiq Ammari, Priya Kumar, Cliff Lampe, and Sarita Schoenebeck. 2015. Managing Children's Online Identities: How Parents Decide

What to Disclose About Their Children Online. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 1895–1904. https://doi.org/10.1145/2702123.2702325

[3] APA. 2013. *Diagnostic and Statistical Manual of Mental Diorders* (5th ed.). American Psychiatric Publishing, Arlington, VA.

[4] Rachel Batchelor, Ania Bobrowicz, Robin Mackenzie, and Alisoun Milne. 2012. Challenges of ethical and legal responsibilities when technologies' uses and users change: social networking sites, decision-making capacity and dementia. *Ethics and Information Technology* 14, 2 (01 Jun 2012), 99–108. https://doi.org/10.1007/s10676-012-9286-x

[5] danah boyd. 2016. Untangling Research and Practice: What Facebook's "Emotional Contagion" Study Teaches Us. 12, 1 (2016), 4–13. https://doi.org/10.1177/1747016115583379

[6] Virginia Braun and Victoria Clarke. 2006. Using Thematic Analysis in Psychology. *Qualitative Research in Psychology* 3, 2 (Jan. 2006), 77–101. https://doi.org/10.1191/1478088706qp063oa

[7] Jed R. Brubaker and Vanessa Callison-Burch. 2016. Legacy Contact: Designing and Implementing Post-mortem Stewardship at Facebook. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 2908–2919. https://doi.org/10.1145/2858036.2858254

[8] Jed R. Brubaker, Lynn S. Dombrowski, Anita M. Gilbert, Nafiri Kusumakaulika, and Gillian R. Hayes. 2014. Stewarding a Legacy: Responsibilities and Relationships in the Management of Post-mortem Data. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, USA, 4157–4166. https://doi.org/10.1145/2556288.2557059

[9] Shelia R. Cotten, George Ford, Sherry Ford, and Timothy M. Hale. 2012. Internet use and depression among older adults. *Computers in Human Behavior* 28, 2 (2012), 496 – 499. https://doi.org/10.1016/j.chb.2011.10.021

[10] Ray Fitzpatrick and Mary Boulton. 1994. Qualitative methods for assessing health care. *Quality in health care : QHC* 3, 2 (jun 1994), 107–13. http://www.ncbi.nlm.nih.gov/pubmed/10137583http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=PMC1055206

[11] Serge Gauthier, Barry Reisberg, Michael Zaudig, Ronald C Petersen, Karen Ritchie, Karl Broich, Sylvie Belleville, Henry Brodaty, David Bennett, Howard Chertkow, Jeffrey L Cummings, Mony de Leon, Howard Feldman, Mary Ganguli, Harald Hampel, Philip Scheltens, Mary C Tierney, Peter Whitehouse, and Bengt Winblad. 2006. Mild Cognitive Impairment. 367, 9518 (2006), 1262–1270. https://doi.org/10.1016/S0140-6736(06)68542-5

[12] Janice E Graham, Kenneth Rockwood, B Lynn Beattie, Robin Eastwood, Serge Gauthier, Holly Tuokko, and Ian McDowell. 1997. Prevalence and Severity of Cognitive Impairment with and without Dementia in an Elderly Population. 349, 9068 (1997), 1793–1796. https://doi.org/10.1016/S0140-6736(97)01007-6

[13] Galen A. Grimes, Michelle G. Hough, Elizabeth Mazur, and Margaret L. Signorella. 2010. Older Adults' Knowledge of Internet Hazards. 36, 3 (2010), 173–192. https://doi.org/10.1080/03601270903183065

[14] Woodrow Hartzog. 2018. *Privacy's Blueprint: The Battle to Control the Design of New Technologies*. Harvard University Press.

[15] Gavin W. Hougham, Greg A. Sachs, Deborah Danner, Jim Mintz, Marian Patterson, Laura W. Roberts, Laura A. Siminoff, Jeremy Sugarman, Peter J. Whitehouse, and Donna Wirshing. 2003. Empirical Research on Informed Consent with the Cognitively Impaired. 25, 5 (2003), S26–S32. https://doi.org/10.2307/3564119

[16] Clare-Marie Karat, John Karat, and Carolyn Brodie. 2005. Why HCI research in privacy and security is critical now. *International Journal of Human-Computer Studies* 63, 1 (2005), 1 – 4. https://doi.org/10.1016/j.ijhcs.2005.04.016 HCI research in privacy and security.

[17] Tom Kitwood. 1997. *Dementia reconsidered: The person comes first.* Open University Press, Buckingham, UK.

[18] Mary Jane Koren. 2010. Person-Centered Care For Nursing Home Residents: The Culture-Change Movement. *Health Affairs* 29, 2 (feb 2010), 312–317. https://doi.org/10.1377/hlthaff.2009.0966

[19] Amanda Lazar, Caroline Edasis, and Anne Marie Piper. 2017. Supporting People with Dementia in Digital Social Sharing. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17*. ACM Press, New York, New York, USA, 2149–2162. https://doi.org/10.1145/3025453.3025586

[20] Peter Alexander Lichtenberg, Michael A. Sugarman, Daniel Paulson, Lisa J. Ficker, and Annalise Rahman-Filipiak. 2016. Psychological and Functional Vulnerability Predicts Fraud Cases in Older Adults: Results of a Longitudinal Study. *Clinical Gerontologist* 39, 1 (Jan. 2016), 48–63. https://doi.org/10.1080/07317115.2015.1101632

[21] Tobias Luck, Francisca S. Then, Matthias L. Schroeter, Veronica Witte, Christoph Engel, Markus Loeffler, Joachim Thiery, Arno Villringer, and Steffi G. Riedel-Heller. 2017. Prevalence of DSM-5 Mild Neurocognitive Disorder in Dementia-Free Older Adults: Results of the Population-Based LIFE-Adult-Study. 25, 4 (2017), 328–339. https://doi.org/10.1016/j.jagp.2016.07.001

[22] G. Madjaroff and H.M. Mentis. 2017. Narratives of older adults with mild cognitive impairment and their caregivers. In *ASSETS 2017 - Proceedings of the 19th International ACM SIGACCESS Conference on Computers and Accessibility*. https://doi.org/10.1145/3132525.3132554

[23] Diane F. Mahoney, Ruth B. Purtilo, Frank M. Webbe, Majd Alwan, Ashok J. Bharucha, Tim D. Adlam, Holly B. Jimison, Beverly Turner, and S. Ann Becker. 2007. In-Home Monitoring of Persons with Dementia: Ethical Guidelines for Technology Research and Development. 3, 3 (2007), 217–226. https://doi.org/10.1016/j.jalz.2007.04.388

[24] Jennifer Mankoff, Gillian R. Hayes, and Devva Kasnitz. 2010. Disability studies as a source of critical inquiry for the field of assistive technology. In *Proceedings of the 12th international ACM SIGACCESS conference on Computers and accessibility - ASSETS '10*. ACM Press, New York, New York, USA, 3. https://doi.org/10.1145/1878803.1878807

[25] Najmeh Miramirkhani, Oleksii Starov, and Nick Nikiforakis. 2017. Dial One for Scam: a Large-Scale Analysis of Technical Support Scams. In *Proceedings of the 24th Network and Distributed System Security Symposium (NDSS 2017)*. Internet Society.

[26] R. J. V. Montgomery, J. G. Gonyea, and N. R. Hooyman. 1985. Caregiving and the Experience of Subjective and Objective Burden. 34, 1 (1985), 19–26. https://doi.org/10.2307/583753

[27] Maurice Mulvenna, Suzanne Martin, Stefan Sävenstedt, Johan Bengtsson, Franka Meiland, Rose Marie Dröes, Marike Hettinga, Ferial Moelaert, and David Craig. 2010. Designing & Evaluating a Cognitive Prosthetic for People with Mild Dementia. In *Proceedings of the 28th Annual European Conference on Cognitive Ergonomics (ECCE '10)*. ACM, 11–18. https://doi.org/10.1145/1962300.1962306

[28] Tobias Nef, Raluca L. Ganea, René M. Müri, and Urs P. Mosimann. 2013. Social Networking Sites and Older Users – a Systematic Review. 25, 7 (2013), 1041–1053. https://doi.org/10.1017/S1041610213000355

[29] Sandra Petronio and Irwin Altman. 2002. *Boundaries of Privacy: Dialectics of Disclosure*. SUNY Press.

[30] Anne Marie Piper, Raymundo Cornejo, Lisa Hurwitz, and Caitlin Unumb. 2016. Technological Caregiving: Supporting Online Activity for Adults with Cognitive Impairments. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, 5311–5323. https://doi.org/10.1145/2858036.2858260

[31] Judith Rodin and Ellen Langer. 1977. Long-Term Effects of a Control-Relevant Intervention with the Institutionalized Aged. *Journal of Personality and Social Psychology* 35, 12 (1977), 897–902. https://doi.org/10.1037/0022-3514.35.12.897

[32] Yvonne Rogers, Jeni Paay, Margot Brereton, Kate L. Vaisutis, Gary Marsden, Frank Vetere, Yvonne Rogers, Jeni Paay, Margot Brereton, Kate L. Vaisutis, Gary Marsden, and Frank Vetere. 2014. Never too old. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems - CHI '14*. ACM Press, New York, New York, USA, 3913–3922. https://doi.org/10.1145/2556288.2557184

[33] Richard M Ryan, Edward L Deci, and Wendy S Grolnick. 1995. Autonomy, relatedness, and the self: Their relation to development and psychopathology. *Ariel* 128, 151.189 (1995), 155.

[34] Supriya Singh, Anuja Cabraal, Catherine Demosthenous, Gunela Astbrink, and Michele Furlong. 2007. Password Sharing: Implications for Security Design Based on Social Practice. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '07)*. ACM, 895–904. https://doi.org/10.1145/1240624.1240759

[35] Sarah Spiekermann. [n. d.]. The Challenges of Privacy by Design. 55, 7 ([n. d.]), 38–40. https://doi.org/10.1145/2209249.2209263

[36] S. Spiekermann and L.F. Cranor. 2009. Engineering Privacy. 35, 1 (2009), 67–82. https://doi.org/10.1109/TSE.2008.88

[37] John Vines, Gary Pritchard, Peter Wright, Patrick Olivier, and Katie Brittain. 2015. An Age-Old Problem. *ACM Transactions on Computer-Human Interaction* 22, 1 (feb 2015), 1–27. https://doi.org/10.1145/2696867

[38] Audrey S Weiner and Judah L Ronch. 2003. *Culture change in long-term care*. Routledge.

[39] Carol J. Whitlatch, Katherine Judge, Steven H. Zarit, and Elia Femia. 2006. Dyadic Intervention for Family Caregivers and Care Receivers in Early-Stage Dementia. 46, 5 (2006), 688–694. https://doi.org/10.1093/geront/46.5.688

[40] Alan Yu. 2016. How a 'Nightmare' Law Could Make Sharing Passwords Illegal : All Tech Considered : NPR. http://www.npr.org/sections/alltechconsidered/2016/07/14/485735920/how-a-nightmare-law-could-make-sharing-passwords-illegal