Building for 'We': Safety Settings for Couples with Memory Concerns

Nora McDonald
University of Maryland, Baltimore County

Helena M. Mentis
University of Maryland, Baltimore County

ABSTRACT

Designing technologies that support the mutual cybersecurity and autonomy of older adults facing cognitive challenges requires close collaboration of partners. As part of research to design a Safety Setting application for older adults with memory loss or mild cognitive impairment (MCI), we use a scenario-based participatory design. Our study builds on previous findings that couples' approach to memory loss was characterized by a desire for flexibility and choice, and an embrace of role uncertainty. We find that couples don't want a system that fundamentally alters their relationship and are looking to maximize self-surveillance competence and minimize loss of autonomy for their partners. All desire Safety Settings to maintain their mutual safety rather than designating one partner as the target of oversight. Couples are open to more rigorous surveillance if they have control over what types of activities trigger various levels of oversight.

CCS CONCEPTS

• **Human computer interaction (HCI)** → HCI design and evaluation methods; Scenario-based design.

KEYWORDS

Memory loss, cybersecurity, scenario-based design

ACM Reference Format:
Nora McDonald and Helena M. Mentis. 2021. Building for 'We': Safety Settings for Couples with Memory Concerns. In *CHI Conference on Human Factors in Computing Systems (CHI '21), May 08–13, 2021, Yokohama, Japan.* ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3411764.3445071

1 INTRODUCTION

Couples facing memory loss are confronted with the challenge of how to manage their online life together safely, as individuals and a pair, while preserving the autonomy of the individual with memory loss. Managing cybersecurity, at any age, is challenging, and it is a concern that many people have—whether or not they are experiencing memory loss [29, 33]. While those who do may ultimately need new kinds of support, the form of support required and preferred may, in fact, have more to do with sociotechnical dynamics than with degree of memory decline [28].

The importance of "couples"' identity has surfaced in the literature as a critical interpretive lens through which to assess appropriate strategies for intervention—strategies that may, in turn, have implications for their sociotechnical partnership. Where before the focus has been on the caregiver burden, scholars of dementia and gerontology are observing the profound importance of collaborative approaches to managing memory loss. Previous research suggests that couples' sociotechnical roles [23] and identities, as they relate to memory loss [15], are both overlapping and entangled. While not necessarily new, the idea that the "maintenance of self in dementia cannot be achieved alone" [14] and that memory loss must be approached as a shared project, not a burden, has still not been fully explored in the sociotechnical realm. To date, very little work has focused on the mutual development of cybersecurity safeguards for couples facing memory loss or MCI.

This paper reports on findings from our scenario-based participatory testing of a Safety Settings application with partners where one or both is experiencing "memory-related concerns." Because deterioration in memory is a pervasive age-related experience and is not necessarily accompanied by a confirmed diagnosis of any kind, our goal for this phase of research was to study people in partnerships who perceive memory loss or have concerns about memory performance, rather than to study people who necessarily have formally diagnosed memory loss. We explore the system as an early "intervention"—a word we borrow from the literature with the understanding that it does not do full justice to the cognitive performance status of these couples, whose ability to evaluate the utility of the system assumes a level of memory competence that might limit their own perspective.

For this qualitative study, we introduced scenarios for our Safety Setting application designed to provide technology choices that empower couples to enhance their security practices with partners. These scenarios situated couples in the everyday features of the Safety Setting design in order to obtain their feedback about how the system communicates. We re-engaged participants who had already worked with our Safety Settings probe in previous research (finding four out of six couples willing to participate again) because familiarity with the settings allowed us to easily bridge from basic utilities to various scenarios, including feelings about surveillance, effort, and autonomy. Couples were asked throughout the interviews whether the scenarios prompted them to change their decisions about their settings. In two cases, preferences did, in fact get reassessed (though not necessarily permanently changed) based on a perception that the system might be too intrusive. In all cases, however, these couples were enthusiastic about the ability to mutually monitor what the other is doing, even independent of concerns about memory loss. They liked the idea of having choice in their selection of Safety Setting levels (e.g., from *recording links*

CHI '21, May 08–13, 2021, Yokohama, Japan

ACM ISBN 978-1-4503-8096-6/21/05…$15.00
https://doi.org/10.1145/3411764.3445071

to requiring *approval for links*) so long as they are able to adaptively fine-tune which of the links impose greater degrees of oversight.

2 RELATED LITERATURE AND FRAMING

2.1 The Role of Couples

Staying online is important to everyone—no less so, older adult couples facing memory loss—and recent research suggests that arriving at ways to extend their secure online participation should be a cooperative enterprise in which both are closely engaged [23, 30]. Researchers like Keady et al. have pointed out the need to focus on couples rather than individuals when studying memory loss and dementia in older adults [24] and the importance of looking at the relationship dynamics to understand individual goals [17, 18]. They argue, along with McDonald et al. [23], that support for dementia should incorporate cooperative approaches that help couples face memory loss as a "team."

More recent research on couples facing dementia suggest that the identity of the partners is often overlapping, and there is some suggestion that, at least for caregivers who are responsible for maintaining some oversight, it is constitutive (or evolving) with the illness [15]. The identity of couples morphs and adapts with cognitive changes that shift responsibilities from one to the other but also redefine the pair as a social unit. Additionally, research emphasizes the importance of relationship-building to counteract the emotional and psychological toll of dementia [3].

In interviews conducted with couples over five years, Hellström et al. find that "sustaining couplehood" is critical for couples coping with dementia. This maintenance involves "talking things through"—even if, over time, some aspects of the work becomes hidden as the other member of the couple becomes more removed [13]. Hellström et al.'s research supports the idea that couples facing dementia put energy into sustaining a "we" that is consistent with the idea of partnership in which both contribute [12, 14]. This "we" can become, over time, a fictional exercise as one partner takes on the responsibility for invisible labor required to maintain the semblance of online autonomy for both.

2.2 The Importance of Not Labeling

Recent research in the inclusive privacy and human-computer interaction (HCI) space focuses on the need to capture non-normative technology experiences when studying privacy. It also encourages accommodation of differences in mobility, vision, and cognition associated with aging as not a problem, per se, but rather, just consideration of the "varying abilities or characteristics" we are accustomed to seeing in all populations [38].

We take an approach to research that is collaborative and meets participants on their own terms in that we do not ask for a specific diagnosis or invite couples to assume labels or roles. Some research has considered privacy in designing support for aging [25, 26], but fewer take a participatory, co-constitutive approach [36]. One example of research that reflects the cooperative nature of privacy among older adults has been explored in Cornejo et al.'s study of content-sharing in the context of art therapy [8]. Their work extends Altman's individual-based theory to consider cooperative negotiation of boundaries in the pursuit of alternative therapeutic interventions. Our methods for research bring a collaborative and non-disability (or non-illness) oriented lens, avoiding the risk of fixing on memory loss as a limitation or label belonging to one individual, rather than a condition that directly implicates others around them and redefines those relationships in complex ways.

2.3 Designing Systems for Older Adults: Autonomy, Privacy, Surveillance, and Collaboration

While technology offers a means for partners and/or caregivers to potentially extend autonomy—for instance, by allowing one partner to monitor the online activities of another for safety—there are important ethical issues that arise from that kind of monitoring inside the home or in institutions [22]. The work of Mahoney et al. emphasizes the importance of respect and autonomy, but also broadens the lens to consider respect for the people assisting and with whom they live [22]. Piper et al. invites ethical concerns around surveillance—for instance, and in particular, with joint accounts [31]. How then should we consider agency alongside surveillance? This question, in fact, invites broader questions about how we view those experiencing cognitive changes.

While shifts in the literature towards personhood highlight the importance of autonomy and respect [21], Bartlett and O'Connor suggest a more sociological view that considers power, agency, and structure [2]. They argue that concepts like personhood, while widely embraced [6], are perhaps too limiting, failing to take into account the larger social issues at play; and that broader concepts of citizenship, while collectivist and sociopolitical, might overstate or misapply notions of agency, which are linked to independent cognition. Another problem with the idea of citizenship is that it is also tied to notions of privileged membership and thus, the potential for exclusion—insofar as it may place a higher priority on keeping order than on tending to the needs of marginalized individuals. One can, however, see the concept of diminished cognitive capacity as a problem of diminished power [2] requiring social change. In their discussion of *critical* dementia, Lazar et al. challenge the very notion of normative cognition to encompass experiences beyond traditional notions of knowledge, which, if valued, help to restore fuller participation in society [19]. This micro-macro resolution (consideration of individual and larger social context) is what Bartlett and O'Connor had in mind.

The authors also share a focus on social forces—in particular, the importance of cooperative work perhaps alongside notions of citizenship to enact social change, and thus, the need to support not merely those with cognitive changes, but also the partners and caregivers whose participation is needed [21]. Other literature, without explicit theoretical agendas, similarly points out that memory concern is "a complex and cooperative social practice" [31] which "couples" do collaboratively [3, 13, 14].

We return, then, to this string of tradeoffs (privacy and surveillance vs autonomy vs safety of the couple) even if we don't resolve them. While conversations about the tradeoffs between, in particular, surveillance vs safety are usefully prompted by citizenship, we might be better off turning to (or at least augmenting with) concepts of social awareness which characterize collaborative environments. Even in this cooperative paradigm, privacy is going to be a central issue. With these rights (whether rights to participation, citizenship,

or some broader sociological construct [2]) comes shifts in the way we view privacy—which must balance the needs of individuals and shared well-being (collective good) of the couple.

2.4 Surveillance Mechanisms

Our work attempts to support couples who are facing the experience of memory loss, and its implications for their cybersecurity through the negotiation of Safety Settings. In this realm, we attempt to provide support for a "team" [15] striving to preserve and maintain deep, shared histories and previously developed sociotechnical roles in the adoption of *surveillance* mechanisms meant to preserve online safety. The Safety Settings application is enabling of, at very least, mutual (or one-sided) oversight of the other's internet activities. At its most restrictive, it requires permission for, or even completely prevents, certain activities.

Studies of older adults and their privacy demonstrate that there is desire for technology that improves autonomy [9] and that older adults may be willing to trade some privacy for autonomy [35]. Yet, research in this space warns of the disconnect between developers who perceive privacy threats as primarily those from without [1] and not necessarily those from within, that could result, for example, from individuals with permissions. While not in the context of dementia perse, this literature speaks to a growing concern for the risks of "dual use" [7] technologies, which require non-normative approaches to design [23].

Studies of dementia which explore the ethical dimensions of privacy note the complex dynamics arising from surveillance in different contexts of care, although the focus is often on caregivers (e.g., [36, 37]). While there are analogs for the dynamics of surveillance among vulnerable users who are being surveilled—for instance, children (e.g., [16, 39]) and in the context of intimate partner violence and surveillance (IPS/IPV) (e.g., [10, 34])—few, if any studies, have looked at the sociotechnical dynamics of older couples facing memory loss when surveillance is involved. Our scenarios were designed to engage participants previously exposed to a Safety Settings probe with the implications of this surveillance—in other words, to make more explicit the daily routines that would be monitored and how, in order for them to fully understand the implications. For this study, we focused significantly less on the prevention of harms associated with cyberthreats, and more on the surveillance and cooperative negotiations among couples.

3 PARTICIPATORY SCENARIO-BASED DESIGN

During this phase of research, we set out to expose couples we had previously studied to a set of scenarios involving the Safety Settings for email. In a previous study [23], couples simply chose from a range of Safety Settings that they would desire for a hypothetical system. In this study, we provide scenarios as context for these Safety Settings. We chose email links for these scenarios for several reasons. First, as a very personal (individual) and relatively frequent activity, email is quite likely to provoke surveillance concerns in the context of oversight burden, creating tensions and potential disincentives for both partners. Second, in our previous research, email was seen as a source of general threat—not necessarily because of the vulnerabilities created by memory loss so much as the vulnerabilities created by careless senders who don't properly vet links or spam. The cross-pressures of perceived need or value and surveillance sensitivities make email an interesting test ground for the tradeoffs association with balancing risk of security vs intrusion.

Scenario-based design is a commonly used method that allows researchers to present contextually rich narratives [32]. We chose scenarios, rather than prototypes, because scenarios invited richer description of several likely futures, which are neither simplistic nor idealistic, and allow description of goals, motives, and context for hypothetical designs [40]. For instance, we wanted to emphasize what it would be like for the system to work while participants were busy doing other things (i.e., what the oversight burden might be) and also in the event one member of the couple were away for an extended period of time and how that might impact alerts (i.e., oversight burden in tension with autonomy).

We took a participatory design approach [11] for several reasons. First, we wanted to continue our frame of cooperative work for couples who stated in previous research that they approach memory loss collaboratively. Second, participatory design acknowledges that the journey of memory loss is uncertain with an approach to system settings designed to accommodate that uncertainty. Finally, scholars have emphasized the importance of using participatory design among marginalized communities, whose perspectives are not well represented in mainstream designs [20, 41]. The elderly qualify, in many respects, especially in the cyber-realm, where terms of their participation are given limited attention.

3.1 Scenario Descriptions

Our system design involves a total of five safety settings that are informed by the issues already identified in previous work where couples are looking for a spectrum of choices that accommodate their sociotechnical needs and respect for autonomy [23, 28, 31]. The situations that we developed based on that prior work were in the context of email, Facebook, online banking or money transfer, online shopping, password management, and online browsing. We tested the following options for each setting: not interfere; record all links clicked on for partner to see later; immediately notify partner of the link clicked on; immediately notify partner of the link clicked on and have them review before continuing; deactivate all links.

This study looks only at Safety Settings for clicking email links. We tested six scenarios for the five safety settings provided. The scenarios used two characters whose personas, image, and names were designed to be gender and race ambiguous. Remi was depicted with grey hair and dark skin and was labeled as a "he." Sydney was depicted with somewhat lighter skin and pink hair and was labeled as a "she." Remi's activities and hobbies included gardening and politics. Sydney's activities and hobbies included grocery shopping, dog walking, and hiking. The goal was less to advance the idea gender fluidity (our couples are heterosexual) on a cultural level, as it was to limit the degree to which any given respondent might project onto any one of the characters, as memory concerns were not gender specific. Remi was depicted consistently as the one with memory issues because switching between the couples was too complicated for a two-hour engagement with dense scenarios.

Scenarios were illustrated and presented in PowerPoint using screenshare. Each scenario was presented with a verbal description

on the left side of the screen and a visual representation of the scenario on the right. The faces of Remi and Sydney came from https://www.iemoji.com/. Sydney was altered to have pink hair to avoid stereotypes of being older had having grey hair. Images of the protype are not shown because no copyright was obtained for the emojis.

3.1.1 Not Interfere. This was the simplest scenario because the Safety Setting system does *not interfere*. We presented participants with a scenario in which Remi receives an email from his plant nursery, Urban Grow, advertising seminars and classes on their blog. In order for Remi to learn more, he is prompted to click a large button in his email saying, "See what we're up to!" Our goal in presenting this scenario was to orient participants to the baseline. We asked couples specifically whether they would want some indication that the Safety System was on, even though they had set it to *not interfere*.

3.1.2 Record all links clicked on for partner to see later. In this scenario, Remi sees an email from a friend (Joe) recommending a gardening video and another one from a friend Bart that's somewhat unclear but suggests it might be about cybersecurity. Notably, in the email from Bart with the subject "Staying Safe!" that says "check this out" the link spells "cyber" incorrectly by omitting the "e." In part 2 of this scenario, Remi sees a pop-up that indicates his links have been *recorded*. In part 3a and 3b, we see Sydney's view which is comprised of two versions of a screen where she can look at what links Remi has clicked on. In 3a, she sees a list of links with email subjects, timestamps, and the actual links. In 3b, she sees the same list but with safety grades (A+ through D+) and a key that indicates what the grades mean. The grades are borrowed from the DuckDuckGo browser, and is based on their ratings including: whether the cite is encrypted, whether all or some of its privacy practices are known, or simply determined to be unsafe. We did not define these ratings for participants but did provide context that DuckDuckGo's ratings notably rate Facebook as C+ to give participants a sense of how to gauge these ratings. Both 3a and 3b state in the scenario text that cyber is misspelled and that perhaps Sydney might need to discuss different safety settings with Remi. This is meant to evoke what reviewing the links entails, opening up the possibility that Sydney might actually need more help in quickly identifying what links to be worried about. This is the only time we attempt to simulate concern.

3.1.3 Immediately notify partner of the link clicked on. In this scenario, Remi sees an email from a friend (Joe) again with the same gardening video recommendation as in the previous scenario. This time, when Remi clicks on the link, he sees a pop-up saying, "Sydney has received a notification that you have clicked on a link." We go to Sydney's view where she is out walking the dog. She receives a text saying that Remi has clicked on a link from Joe, with the email subject, "Gardening video" and a link to a YouTube video. In alternative scenario, she receives a phone call from "Safety Settings" with this information presented by an automated voice.

3.1.4 Immediately notify partner of the link clicked on and have them review before continuing. This scenario incorporates two scenes meant to build tension around response burden, immediacy, autonomy, and safety. We manipulate whether Sydney has able to easily respond, whether Remi has to wait for a short or long period of time, and we add pressure by making the type of activity one that provokes more or less fear. We used a political donation scenario that made the stakes a little higher, since couples remarked in previous research that money issues garner more concern. We then use a YouTube scenario that we thought might seem safer.

In scene 1, Remi receives an email from a Senator that looks like a candidate he supports. It has a sense of urgency and is also specific to Remi's area code. It contains a link to donate $5. When Remi tries to click on this link, however, he is directed to a screen that asks him to verify that he would like his partner to review the link to the donation site (act.com/donate) or cancel and not proceed. Remi decides to proceed and is directed to a page where he is told to standby while his partner reviews the link he wants to click on. Meanwhile, Sydney is pictured at the grocery store in the checkout line when she receives a text alerting her to the fact that Remi has clicked on a link and would like it to be reviewed. She is asked to indicate whether the link is safe, or not, by responding "yes" or "no" in text. An identical scenario involving a phone call is also shown where Sydney is instructed to select "1" for "yes" and "2" for "no." In the narrative that follows, Remi is made aware that his link has been approved via a text and when the screen refreshes. The options to proceed from these locations as well as the original email are demonstrated to participants to evaluate what is a plausible set of steps. The screen Remi goes to is a campaign for the cartoon character Snoopy. On this donation site, one can donate upwards of $5 dollars (amounts specified include $20, $50, $100, $200, $500, $1,000 or some other amount).

Sydney then receives another text asking her if she would like to approve all links to this act.com/donate website so that Remi doesn't have to go through this process again. (Participants were also verbally asked if they would also want to approve all links from a specific sender, in addition to for a specific website). Sydney says "no" to approving all links from this act.com site. We then provided a recap screen that shows what happens in the future when Remi is not able to simply proceed with links from act.com.

In scene 2, Remi receives an email from his friend Ellis telling him to check out something "hilarious" with a link to a YouTube site and nothing else to indicate what it's about. This is meant to stir up some light concerns about the authenticity of the link and/or sender; at the same time we imagine that many communications are this cryptic between friends. Remi wants to click on the link but is sent to the same series of screens where he must indicate he wants his link approved and then wait for approval.

This scenario heightens tensions around response burden, immediacy, autonomy, and possibly safety. In this scenario, Sydney is on a hike and, presumably, less easily disturbed. She sees a text alerting her that Remi would like her review but wants to wait. This "lag" is meant to evoke tension around Remi and Sydney's desire for safety and the need to wait for approval from Sydney (loss of autonomy for Remi) or have Sydney respond (response burden and loss of autonomy for her). It is not until three hours later that Remi finally receives approval for his link. We then re-introduce the narrative in which Sydney is asked to *approve all links* from this website (which, in this case, is YouTube). This is meant to create tension between the desire to not leave the other hanging, the desire to not be disturbed while doing relaxing or recreational, and the pressure

to provide blanket approval to a site that is harmless but also vast. Sydney decides to approve all links from YouTube, so that the next time Remi receives an email from YouTube, he can click on it without getting approval. We asked in the interview for couples to talk about how they felt about that decision.

3.1.5 Deactivate all Links. In the final scenario, participants are shown Remi receiving the same email from act.com/donate as shown in the previous scenario, only this time, when he tries to click on the link, he is shown screen that says that email links are deactivated and that he should try forwarding the email to his partner to discuss together.

3.2 Scenario Presentation

Couples that participated in this study were shown the Safety Settings previously tested and asked if they remembered them, but were not shown their previous answers. They were told that they would be shown scenarios pertaining to each Safety Setting and could make adjustments throughout—again, with no indication of what they had previously chosen. For each slide, the narrative descriptions that were used to illustrate each Safety Setting scenario were provided on the left and the visual representation of these scenarios (e.g., a depiction of an email screen, a pop-up, an iPhone message, etc.) were provided on the right. Couples were told that each scenario would be read and the visual read and described. A progress bar was shown on the upper right-hand corner of each slide.

Couples were then introduced to Remi and Sydney as the characters who would be depicted in each scenario; no backstory was provided. Couples were instructed that the exercise was designed to get their feedback and as a participatory design session they were encouraged to comment on design decisions and even envision entirely alternative ways of depicting settings. Each scenario was introduced with a reminder of the Safety Setting being used. To encourage participatory engagement, we asked couples to tell us if the design was intuitive and if they would change anything about the design or content, and also how they might want information communicated, their ideas for how to provide Safety Settings for email links and other worries not covered by these scenarios and how to address them. Couples were adept at thinking through where they might get a text and what they might do in those instances as well as what information they would need to make decisions.

As mentioned, since couples had already been through a previous study where we asked them about what Safety Settings they would use in various contexts (i.e., email, Facebook, online banking or money transfer, online shopping, password management, and online browsing) we also asked them if they felt they were more or less likely to use a setting know that they had seen how a scenario might play out.

3.3 Study Participants

Participants were recruited in July, 2020 (during the COVID19 pandemic) from among those we had previously interviewed in our study of the Safety Settings probe, all of whom were drawn from a market research panel. We sent emails to all six panel couples with a request to participate in follow-up research with Safety Setting scenarios, represented as two-hour long participatory sessions. Four out of the six agreed to participate. We have developed relationships with these couples over the course of the past year. While we do have a sense of who is suffering, at all or more, our approach was to not impose labels or roles and thus we do not request a specific diagnosis. Couples were given a $37 honorarium. In our reporting of results, we refer to participants interchangeably as couples and Negotiating Partners (NPs). Our research was approved by our institutional regulation board.

3.4 Analysis

Interviews were audio/video recorded and transcribed using a video conferencing system and edited manually. The first author conducted the participatory sessions and took notes during those sessions. The first author wrote memos and reviewed transcripts (and manually edited them) after each interview in an iterative process that produced themes as they pertained to design (including features, content, and alternatives to scenarios) and concerns about surveillance, as well as surfaced themes previously identified like the paradoxical importance of self-surveillance and surveillance to maintain autonomy and because of the uncertainty of progression [23]. This process most closely resembles a mixed deductive and theoretical thematic analysis approach [4, 5]. However, we take a phenomenological stance, privileging the realities and apprehensions of participants, regardless of whether they are, in any given situation, "correct" about their safety. We organized our findings around Safety Settings scenarios and also touch on inductive themes.

4 FINDINGS

4.1 Not Interfere

Couples found the do *not interfere* scenario acceptable but wondered what might happen if the link were less benign. In our discussions, we learn that there are, indeed, times when they would want the system not to interfere with links they designate as safe (e.g., a routine service provider or church) or under circumstances when they prefer or require total privacy—for instance, if buying a gift for the other partner.

4.2 Record All Links Clicked for Partner to See Later

Consistent with our previous research, couples very much liked the *record* all links scenario because it gives them the ability both to keep an eye on what the other is doing and also gives them the ability to retrace their own steps. In fact, one participant noted that they use the history in their browser to effectively do the latter:

> "I always keep history on because I never know what I need to look for something." [NP2-1]

One couple, in response to our intentional misspelling of the word "cyber" in a link, feels that this history was useful, even while pointing out that this is something they have always been looking for and which comes up with friends:

> "Well, I love the idea of recording the links myself, because in this case . . . You know, it's not legitimate because anytime there's a misspelling in the in the link of word, or whatever, there are some suspicious

> something behind the scenes. That's always been a discussion for everybody." [NP3-1]

NP3 likes the logs because, regardless of memory loss, the "average person" (including their spouse with memory loss) may not know to look for misspellings. The implication is that this could be a challenge for anyone.

> "But the average person I mean, my husband may not know that to look at these address and know that, OK. That's misspells. And now so I'm not going to click on that." [NP3-1]

When shown the Firefox pop-up alert telling them their link had been *recorded*, couples do express concern about the presentation. It made them think that it was Firefox or some other company, and not the Safety Settings, that had recorded their links.

> "It could be reported by a website, by an e-mail company, or by anybody. I always figure more information is better. And if I saw that saw that, I might be alarmed. Somebody is recording me." [NP1-2]

For this reason, NPs recommend making the language more explicit or using the Safety Settings logo, because otherwise they would be nervous that it was some other company taking their data. One couple has no problem with the pop-up alert but wants to make sure they don't have to engage with it because it would distract them from what they are doing:

> "That's fine as long as I don't have to click it to say, I saw it . . . I don't mind the message as long as it, you know, it'll stay for five seconds. Give me the option to change how long it appears on the screen and then let it go away." [NP2-2]

When NPs are shown the screens representing the list of *recorded* links, they find it clear and intuitive. They like the idea of recording links, in particular, because they have been shown a scenario in which one of the links was misspelled. One couple adds that "the review should turn up [those] problems" [NP3-1]. This same couple points out that even though memory loss is not an issue now, they like to keep an eye on each other's activities to ensure they are safe:

> "It's very reasonable. Very easy to understand." [NP2-2]

> "And I'll always keep it on just to have a track back in case something. Okay." [NP2-2]

Couples say they regularly confer about links they receive in email to make sure they are okay and that they *both* like it to be able to retrace their own steps.

4.2.1 Grading Links. Couples do express preference for the screen which includes a grading of the links according to their privacy practices—though they want more clarification on the criteria. They do express slight reservations about just having a rating system without also being able to override it because there are some sites they visit which they know to be safe but that they suspect a rating system might consider not safe.

> "I love it. My initial questions are, though. I mean, who decides what criteria is used for determining the ratings? Because some sites that I may go to, may say, 'oh, wow, that rating is not safe.' It's unsafe. But it really is due to the current situation that we live in and in the world. You know, people have different perspectives about what they deem as safe and unsafe, you know?" [NP3-1]

This desire for their own subjective judgements leads couples to say they also want the ability to determine what links are safe or not in some formal way. NP3 expresses that safety is relative and for them, as for others, it makes sense to ask to decide based not just on safety rating but on the business or sender what Safety Settings should apply.

NP1 extends the ratings design further and points out that these ratings might have been helpful for Remi before he clicks on an email, which echoes couples' sentiment that these ratings have other uses for customization and for behavior:

> "But it would also be helpful if Remi got that information when he got the e-mail so that he might not want to click on that." [NP1-1]

One couple specifies that they would want to use the *recorded* links log interface to click what links they would like to eliminate from the unsafe list, as well as links to which they would want to attach more rigorous settings. In essence, the *recorded* link logs provide what they see as a useful dashboard from which to manage Safety Settings, allowing them to identify problem links and assign them to stricter settings like immediately notify, review, or deactivate; cull the list of links that are deemed safe/unsafe; and delete links from sites that maybe they want generally recorded but not in that instance (e.g., when they are buying a gift). They feel that a grading system or some type of alert might be used to preempt troublesome links. For instance, some system that would trigger a review, even if the couple's default setting was *record*. Another couple envisions a version of this where a troublesome link triggers a warning sign for the partner, rather than an alert for review:

> "I like a stop sign or something that would come up with question mark or something like that." [NP1-1]

NP2-1 likes the grades because it mimics an aspect of their sociotechnical dynamic but allows them to avoid bothering the other partner:

> "I'm always checking for safety because you never know what you're going to get in the mail and I usually just pass an email an email to him and say, should I open this? So, this would be better for me. I don't have to bother him." [NP2-1]

Ultimately, the link grades or ratings have several functions that couples imagine through participatory engagement: triggering an alert for couples before they click on a bad link or giving them insight into whether or not to click; allowing them to identify what links that have been clicked might be bad; and later as a way of designating stringency of Safety Settings attached to a link.

4.3 Immediately Notify Partner of The Link Clicked On

This scenario *immediately* showcasing the Safety Setting notification (by phone or text) that the partner has clicked on a link is one that garners consistent enthusiasm. The pop-up appearing for Remi, which specifies that "Sydney has received a notification

that you have clicked on a link," is found to be very clear. Before couples had indicated they wanted a Safety Setting logo associated with the pop-up to understand what was recording their links, but the additional language specifying that links are being immediately communicated to the partner seems to satisfy this desire for certainty.

One couple initially worries that these *immediate* notifications might be overkill, but after seeing the text message alerting Sydney to the links Remi has clicked on, they deem it convenient and "attractive" [NP3-1], particularly if the rating system can be used to "filter" what they see. Another (straying from just the email scenario) worries that it might get annoying if someone is "surfing" the web:

> We don't see a problem with it, except if someone is surfing, surfing the net and clicking on a lot of things, you need to get a lot of notifications. That would be the only downside. [NP1-1]

Another couple, talking about the need to have a way to white list certain sites by hand:

> "I would like to be able to say, OK, this is a safe site. So. I would like to have some say into on a personal level, I don't know if this is just going beyond the realm of this project, but if there is a site that I go in all the time every week to make an appointment, to get my nails done, of course, at sites say so, I would like to have some type of input myself to say, oh, OK, this is a safe site . . . It's a combination of both because, me, I wouldn't wanted to junk up my system, and also, I mean, I've deemed this site to be safe." [NP3-1]

This couple, NP3, while they like the *immediately notify partner* scenario, is also concerned about Facebook advertising as well as scams and phishing from other unknown sites that may be delivered by trusted senders:

> "Especially if it could be a virus attached to something information or if it's a bogus site, say, on Facebook, you see some advertised and you wanted to order the item. And you didn't have to make sure it wasn't a scam. No, I tell you what, somebody indicated the site to stay away from and not go to that site." [NP3-1]

This sentiment is also shared by NP1 and NP2. Couples mention the fact that certain spam just can't be eliminated, and that clicking on unsubscribe has the inverse effect of leading to more spam. They perceive that this mechanism could serve as an additional spam filter:

> "So, even if you stop the one [subscription], I swear they send it out and you can get tenfold for trying to quit. I am currently getting emails for a woman named [Kathy]. I click unsubscribe and it just gets worse." [NP1-1]

Couples want help managing noise and potential threats, and the specific relevance of memory concerns to that objective is not always clear. Independent of memory issues, there can be slightly divergent views within a couple regarding the role each would want to play in monitoring those intrusions, sometimes reflecting historical roles and perceived competence to scrutinize to surveil, unrelated to memory. In some cases, the partner with greater memory loss may be the one more adamant about reviewing the other partner's links.

Notably, couples emphasize throughout that for them personally, calls are not welcome, insofar as calls are strongly associated with spam and bots. At the same time, they believe it should be an option provided by Safety Settings in case someone else might prefer to get contacted that way.

4.4 Immediately Notify Your Partner of The Link And Wait for His/Her Review And Response to Proceed

We provided couples with two sub-scenarios for the *immediately notify and review* scenario. For the first sub-scenario, Remi clicks on a link and is asked if he wants Sydney to *review* the link. He is then instructed to standby while she *reviews* it. Sydney then receives a text or call asking her to *review and approve (or, as we wrote it: "wait for his/her review and response to proceed")* the link Remi would like to view. Once it is approved, Remi's screen refreshes and he receives an alert via text that his link has been *approved.*

For the first scenario: the burden of response is not too great while standing in line for groceries, and Remi's autonomy is not undermined because what's at issue is a political donation, which requires consideration and does not necessarily qualify for a repeating permission (e.g., approve all future donation links).

NP4 is initially turned off by this scenario because they worry that it limits the autonomy of the other:

> "He doesn't like to be told what to do on a daily basis. Like, he can follow the rule of don't click on any link. But if he had to check with me, he does not like to check with me on everything he does." [NP4-1]

NP4-2 reiterates that he has a system for going to the website itself to avoid clicking on links.

> "If I get a link from my doctor's office that says, 'you have an appointment' I don't go to that link. I go to my doctors office [NP4-2]

At one point, NP4-2 says outright their misgivings about the *review* settings making them feel like the other partner "had all the control":

> "No, I wouldn't like feeling like she had all the control." [NP4-2]

Couples find the intermediate screen, where Remi indicates whether to proceed or not with the review, confusing and unnecessary. One couple suggests that it might be a lot to do for a link, though potentially relevant for more advanced conditions:

> "I do. I think, however, that for an older person, it's a lot of information for them to take in. You basically have the email, the wait for the part review, and the access site from your box on the left. I think for older people, if you had a way to simplify it, I find it easy to follow. But I'm wondering if your clients or people with dementia and Alzheimer's, whether that will be more the process." [NP1-1]

The idea of the page refreshing to alert Remi that the link has been approved concerns one couple (NP1), who worry that the

cache might not refresh or that something could be amiss. Thus, they want the text "to be sure" [NP1-2] that the link is *approved*. This scenario shows an email in which the political campaign asks for a $5 donation, but the ultimate screen that Remi is able to access asks for donations of different amounts ranging from $5 to $1,000 and some "other amount." This puts couples on alert because this is precisely what they worry about most—complex choices and signals that might suggest an untrustworthy solicitation. One couple observes that for political solicitations specifically, they would want them deactivated "after November" [NP3-1]. Again, we see a strong desire to adapt all these settings across the full range of options based on context as well as personal preference.

For the second scenario: the burden to respond is greater while hiking and we impose a 3-hour lag, Remi's lack of autonomy is heightened because it's simply a fun, casual YouTube link, but it might also be a more safe site than a political donation, thereby increasing the desire to find an easy fix (e.g., approve all future YouTube links) might be greater.

The lag between when the *request for approval* is sent and when Sydney is able to *review and respond* doesn't really strike couples as a problem. In fact, NP3 points out that if Remi really wants Sydney to review a link, he should call and interrupt her hike. NP1 suggested the option of allowing Sydney to indicate to Remi that she needs more time to review via the text system.

We had anticipated that couples would be more likely to want the ability to approve the link in the future, without having to review it because this might grant more autonomy around trusted sites associated with more casual social interactions, where delays disrupt the cadence of participation. Ultimately, couples have mixed feelings about specifying for which links or senders they might require review.

4.5 Deactivate All Links

When shown this scenario in which Remi simply cannot access links sent in email, couples are hard pressed to think of links they would want to *deactivate*. They do feel that this would be a utility for them both, as a way to block spam more than way to restrict or supervise their partner. Some reference forwarding to their partner as a step they already take and note that some additional encouragement or facilitation would be welcome.

> "Yeah, I mean, and I'm not I'm not the technical brains of this operation, so I don't know if that can be done. That's a great idea." [NP4-1]

> "Yeah. Click here to forward the email to you to discuss together." [NP4-2]

> "I'm always checking for safety because you never know what you're going to get in the mail and I usually just pass an email an email to him and say, should I open this? So, this would be better for me. I don't have to bother him." [NP4-1]

Couples would like a button with which to share questionable links with their partner, but one indicates the desire for some mechanism for customizing links to deactivate when appropriate:

> "If it's after November, whenever the election is, I would put a message in there, after November 15th deactivate this link because no one should be trying to get money." [NP3-1]

4.6 Review and Approval Maybe Not for Us, But Maybe for Other Vulnerable Groups?

Throughout our interviews, we noted themes that pertain to level of comfort with surveillance; concerns tend to arise when the Safety Settings go outside the space of self-surveilling configuration (e.g., beyond logs) or couple's existing sociotechnical fixes (e.g., reviewing and approving as opposed to mutually reviewing). Two of the four couple views logging as the upper bound in terms of Safety Settings surveillance but can imagine vulnerable populations who might benefit: their own grandchildren children, children with autism, or a caretaker for someone with dementia.

NP-3 sees the review and approve scenario as consistent with what they already do:

> "If it happens now, my husband will be on the computer. Oh, his tablet doing something and he's not sure, he'll come to me . . . 'Look at this. Do you think this is a legitimate?"' [NP3-1]

But they also note that they might want to filter out links they feel are safe:

> "No, I wouldn't want to review because I know my church .... I mean I mean they text all the time now. I mean, they set up e-mails all over town now because we all, you know, stuck in the house . . . And I trust them." [NP3-1]

Another couple similarly describes the collaborative workarounds they currently have for situations deemed unsafe as working well:

> "Not for myself. I sometimes either hold off on doing that and ask him. Do you think we should donate to this? But I remember to ask that if I have a hard time remembering it, I might forward him the email. So, it's kind of resembles what I'm doing." [NP2-1]

This same couple, however, would want this system perhaps for their grandchildren (and would have wanted it for their children:

> "I like it because we had gone through the years with computers with our children, but they didn't, they weren't computers until they were almost in high school or college. And this would have been better to keep track of things when it was all new, will the cyber space things and I think it's good for a parent or grandparent to know what sites a child's more. [NP2-1]

NP2-1 notes that because this system offers something that is more immediate, it is tempting for them to endorse, but again, reverts to the idea that this might be appropriate for grandchildren rather than "between partners" [NP2-1] :

> "If I had children or grandchildren, yes, I would definitely want it. For just my husband and I, I might I might even call him and say, should I do this? That's just my opinion for that. [NP2-1]

Later, NP2-1 points out that for consenting adults that the *deactivate* setting might just not be "fair" for adults, but makes sense for a child:

> "If they're both adults, that's not necessarily fair. That's something they should discuss before it's done. If it's a child. I would definitely understand it."

NP2-2 reiterates that they want to maintain their autonomy and thus would not want this level of intervention, but feels that they would only use the immediate settings if their grandchildren were to use their computers:

> "I'd rather check myself, but I look at it if children or grandchildren would use our computers." [NP2-2]

At one point, NP4 considers that this might be useful for a caretaker. The implication being if things get that bad then the person will be vulnerable like a "child":

> "The care takes care of that should have controlled. Just like, if it were child." [NP4-1]

NP4-1 considers that this setting is helpful, in theory because they, as a couple, are so wary of clicking links they employ a "code word" [NP4-1], but feel this should really be for caregivers.

> "Review that means you can't do it until but it helps both couples . . . If they have to help, you're helping to caretake." [NP4-1]

NP1-1 describes how links on Facebook to business that are scamming people are dangerous specifically for those on the autism spectrum.

> "I know a lot of people with children on the autism spectrum and they're using the Facebook and say they're not necessarily questioning what they're seeing." [NP1-1]

NP4 has reservations about immediate notifications but not because of surveillance and because they worry that any system that would be alerting them of threats would be too late.

> "Well, personally, I would never click on any of the link, unless I see who it's from." [NP4-2]

> "My thought is, it's too late once he's already go on there. [NP4-1]

NP4-2 is particularly adamant that he doesn't click on anything because of concerns about safety and just goes directly to the website, to the legitimate source.

5 IMPLICATIONS FOR DESIGN

Previous research suggested that couples want a range of choices for securing cybersecurity in the face of memory loss [23, 27, 28]. This research explored with couples what those settings might mean and how they might work by invoking scenarios that placed safety settings in the everyday context – inviting couples to consider how type of threat and ongoing daily activities might reshape or rebalance their priorities. We found that couples are motivated to use a variety of safety settings if they are able to assign risk to particular activities. We note that two couples do not want the system to surveille the other partner and that other two want to customize that surveillance.

From these sessions, we learned that some couples are wary of (or even against) surveillance for them but might be okay with children; want an indication of link safety before they click on it, or the ability to customize which links trigger more aggressive Safety Settings (i.e., alert or review); and want a system that reinforces already established security behaviors that has them sharing and reviewing collaboratively any links that raise concern.

Our results suggest that the Safety Settings themselves must provide a spectrum of choice—the ability to adaptively decide what forms of digital outreach constitute threats is essential to this system design. Operational preferences may differ—couples may want either to log all links or immediately notify partner—but what's most important to them is customization.

Partners' reticence to label the other as having a memory issue and their sensitivity to the inherent dynamism of their situation (they were explicitly mindful in prior research that tables might turn) are consistent with their emphasis on the relevance of Safety Settings for mutual oversight only. At the same time, many of the objectives they prioritize are rooted in more general cybersecurity concerns which, while perhaps sometimes heightened by memory issues, also exist independently. Mutual review (which some already appear to be doing offline) is not necessarily seen as a bulwark against forgetting so much as a backstop against error. We know from this research that fears about the risks and ramifications of memory loss is perhaps best supported with logs. Alerts and review steps should be approached cautiously, with sufficient ability to customize so that neither the burdens of oversight nor the challenges to autonomy are excessive.

Concerns about surveillance of one another are evident when we present couples with scenarios beyond logs, which strike some as suggestive of the sort of oversight appropriate for children rather that adult partners. For the couples who are willing to accept some modicum of oversight, customization to one degree or another is of paramount importance—a condition of acceptance. We note that for couples with the capacity to assess the utility and acceptable of a system like this, efficacy of collaboration would appear to be a higher priority than efficacy of oversight. For couples dealing with more advanced cases or memory decline, the same priorities cannot be assumed.

Our participants do pick up on the dual use potential of these technologies—i.e., their capacity to both restrict their activities and provide greater autonomy. They believe that for someone who requires custodial care (a child or someone with very advanced dementia) such technologies may be appropriate; for their personal situation, however, such intrusions and technological oversight cross the line. There are limits to this insight, however. Couples don't worry (in these discussions) about the implications for mutual surveillance. But we contend that the limits of their imagination in what appear to be strong, trusting relationships should not have bearing on the obligations of designers. Designers have a broader sightline and can further tap the perspectives of varied stakeholders. Expanding designers' sightline will require engaging with other vulnerable populations (e.g., children and IPV victims).

In the following sections we talk about some iterations to the design that we formulate from our participatory sessions. These implications must be balanced with our understanding of the risks

experienced by other types of vulnerable users and future research should address these gaps.

5.1 Default Mutual Oversight

When we first decided to design this app, it was with the expectation that couples would designate one person who had oversight over everything. While couples sometimes tacitly acknowledged that one might have oversight, they seem to assume that they might mutually share roles as those who receive immediate alerts or as reviewers. This system must be default mutual oversight.

5.2 Record Management Combined With Grading for All Settings

Based on couples' feedback, we did iterate on a record links log page that allows couples to decide how to designate a link across each of the safety settings. For example, we could allow couples to designate links based on the grade given (or some other criteria that comes from their subjective experience with this site). Importantly, it also allows couples to delete links they don't want the other to know they have clicked on (like to shopping sites in case they are buying gifts, which was raised as a concern in this and previous studies). The idea is that we use the record link space to designate a link as one to be secret (delete) or to some other level of review. For instance, couples could assign links to *immediately notify* or *review and approve* links based on their rating. We could also include in this text message the option to designate a link to any of the settings. This is something to explore. Of course, couples could designate links they haven't seen to a review category based on grading and then adjust them in the record/log interface as needed.

5.3 Reiterate off-App Collaborations

Couples frequently remarked that they pursue their assessments of safety through manual ("over the shoulder") review and use of code words. They say, for instance, if there were a lag between when they sent a link for review by the other partner then they would just call them and ask. There may be a need to build into the app suggestions that couples regroup, perhaps, even at the moment they are considering changing their settings as yet another intermediary step. In addition, couples want a button that mimics their sociotechnical dynamic in which they share links they are suspicious of. If a couple has designated a link *deactivate* they may still want to review and the system could support this activity with an affordance that makes the interaction more accessible.

6 CONCLUSIONS

We enlisted couples with whom we have an established relationship to engage in a participatory design session. This approach provided an opportunity to *extend our understanding* of what couples deemed optimal Safety Settings based on a comparison with their recollections of previous responses through an exercise that tested preferences against contextually-rich scenarios. We learned that couples value most the idea of controlling specific vectors (in this case, links and senders in email) through records or logs and immediate alerts, but are very hesitant to adopt Safety Settings that exceed what they already attempt to accomplish by accessing browsing histories and conferring with each other about links that look unsafe. We discovered from this follow-up research that more detailed scenarios enabled couples to think more specifically about the ramifications of various settings and made them even more reluctant to accept surveillance settings that appear to shift the balance of power in the relationship or deprive partners of a sense of agency. Couples maintain that memory loss is a team effort and are careful about assigning the role of oversight to one partner. Security is a shared project, at least for the time being—one that requires collaborative and adaptative solutions. Attempts to enhance security are most appealing when they appear to honor and perpetuate existing roles rather than substantially alter them.

ACKNOWLEDGMENTS

The work is supported by the National Science Foundation grant CNS-1714514.

REFERENCES

[1] Alkhatib, S., Waycott, J. and Buchanan, G. 2019. Privacy in Aged Care Monitoring Devices (ACMD): The Developers' Perspective. Studies in Health Technology and Informatics. 266, (2019).
[2] Bartlett, R. and O'Connor, D. 2007. From personhood to citizenship: Broadening the lens for dementia practice and research. Journal of Aging Studies. 21, 2 (Apr. 2007), 107–118. DOI: https://doi.org/10.1016/j.jaging.2006.09.002
[3] Bielsten, T. and Hellström, I. 2017. A review of couple-centred interventions in dementia: Exploring the what and why – Part A: Dementia. (Nov. 2017). DOI: https://doi.org/10.1177/1471301217737652
[4] Braun, V. and Clarke, V. 2019. Reflecting on reflexive thematic analysis. Qualitative Research in Sport, Exercise and Health. 11, 4 (Aug. 2019), 589–597. DOI: https://doi.org/10.1080/2159676X.2019.1628806
[5] Braun, V. and Clarke, V. 2006. Using thematic analysis in psychology. Qualitative Research in Psychology. 3, 2 (2006), 77–101.
[6] Brooker, D. 2006. Person-Centred Dementia Care: Making Services Better. Jessica Kingsley Publishers.
[7] Chatterjee, R., Doerfler, P., Orgad, H., Havron, S., Palmer, J., Freed, D., Levy, K., Dell, N., McCoy, D. and Ristenpart, T. 2018. The Spyware Used in Intimate Partner Violence. 2018 IEEE Symposium on Security and Privacy (SP) (May 2018), 441–458.
[8] Cornejo, R., Brewer, R., Edasis, C. and Piper, A.M. 2016. Vulnerability, Sharing, and Privacy: Analyzing Art Therapy for Older Adults with Dementia. Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing (San Francisco, California, USA, Feb. 2016), 1572–1583.
[9] Demiris, G., Rantz, M., Aud, M., Marek, K., Tyrer, H., Skubic, M. and Hussam, A. 2004. Older adults' attitudes towards and perceptions of "smart home" technologies: a pilot study. Medical Informatics and the Internet in Medicine. 29, 2 (Jun. 2004), 87–94. DOI: https://doi.org/10.1080/14639230410001684387
[10] Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T. and Dell, N. 2018. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. (2018), 1–13.
[11] Greenbaum, J. and Kyng, M. eds. 1991. Design at Work: Cooperative Design of Computer Systems. CRC Press.
[12] Hellström, I., Nolan, M. and Lundh, U. 2005. Awareness context theory and the dynamics of dementia: Improving understanding using emergent fit. Dementia. 4, 2 (Jun. 2005), 269–295. DOI: https://doi.org/10.1177/1471301205051096
[13] Hellstrom, I., Nolan, M. and Lundh, U. 2007. Sustaining 'couplehood': Spouses' strategies for living positively with dementia. Dementia. SAGE.
[14] Hellström, I., Nolan, M. and Lundh, U. 2005. 'We do things together': A case study of 'couplehood' in dementia. Dementia. 4, 1 (Feb. 2005), 7–22. DOI: https://doi.org/10.1177/1471301205049188
[15] Hernandez, E., Spencer, B., Ingersoll-Dayton, B., Faber, A. and Ewert, A. 2019. "We are a Team": Couple Identity and Memory Loss. Dementia. 18, 3 (Apr. 2019), 1166–1180. DOI: https://doi.org/10.1177/1471301217709604
[16] Jørgensen, M.S., Nissen, F.K., Paay, J., Kjeldskov, J. and Skov, M.B. 2016. Monitoring children's physical activity and sleep: a study of surveillance and information disclosure. Proceedings of the 28th Australian Conference on Computer-Human Interaction (Launceston, Tasmania, Australia, Nov. 2016), 50–58.
[17] Keady, J.P. 1999. The dynamics of dementia: a modified grounded theory study. University of Wales.
[18] Keady, J.P. and Nolan, M. 2003. The dynamics of dementia: working together , working separately , or working alone? Partnerships in family care: Understanding the caregiving career. 15–32.

[19] Lazar, A., Edasis, C. and Piper, A.M. 2017. A Critical Lens on Dementia and Design in HCI. Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (New York, NY, USA, 2017), 2175–2188.

[20] Lindsay, S., Jackson, D., Schofield, G. and Olivier, P. 2012. Engaging older people using participatory design. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (Austin, Texas, USA, May 2012), 1199–1208.

[21] Madjaroff, G. and Mentis, H. 2017. Narratives of Older Adults with Mild Cognitive Impairment and Their Caregivers. Proceedings of the 19th International ACM SIGACCESS Conference on Computers and Accessibility (New York, NY, USA, 2017), 140–149.

[22] Mahoney, D., Purtilo, R., Webbe, F., Alwan, M., Bharucha, A., Adlam, T., Jimison, H., Turner, B. and Becker, S. 2007. In-home monitoring of persons with dementia: Ethical guidelines for technology research and development. Alzheimer's & dementia: the journal of the Alzheimer's Association. 3, (Aug. 2007), 217–26. DOI: https://doi.org/10.1016/j.jalz.2007.04.388

[23] McDonald, N., Larsen, A., Battisti, A., Madjaroff, G., Massey, A. and Mentis, H. 2020. Realizing Choice: Online Safeguards for Couples Adapting to Cognitive Challenges. (Virtual Conference, Aug. 2020).

[24] McGovern, J. 2011. Couple meaning-making and dementia: challenges to the deficit model. Journal of Gerontological Social Work. 54, 7 (Oct. 2011), 678–690. DOI: https://doi.org/10.1080/01634372.2011.593021

[25] McNeill, A., Briggs, P., Pywell, J. and Coventry, L. 2017. Functional privacy concerns of older adults about pervasive health-monitoring systems. Proceedings of the 10th International Conference on PErvasive Technologies Related to Assistive Environments (Island of Rhodes, Greece, Jun. 2017), 96–102.

[26] McNeill, A.R., Coventry, L., Pywell, J. and Briggs, P. 2017. Privacy Considerations when Designing Social Network Systems to Support Successful Ageing. Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (Denver, Colorado, USA, May 2017), 6425–6437.

[27] Mentis, H.M., Madjaroff, G., Massey, A. and Trendafilova, Z. In submission. The Illusion of Choice in Discussing Cybersecurity Safeguards Between Older Adults with Mild Cognitive Impairment and Their Caregivers. Proceedings of the ACM Conference on Computer-Supported Cooperative Work & Social Computing (In submission).

[28] Mentis, H.M., Madjaroff, G. and Massey, A.K. 2019. Upside and Downside Risk in Online Security for Older Adults with Mild Cognitive Impairment. Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (New York, NY, USA, 2019), 343:1-343:13.

[29] New Pew Research Study: A Majority of Americans Know Little About Digital Security and Privacy: 2019. https://www.cpomagazine.com/cyber-security/new-pew-research-study-a-majority-of-americans-know-little-about-digital-security-and-privacy/. Accessed: 2020-07-20.

[30] Piper, A.M., Cornejo, R., Hurwitz, L. and Unumb, C. 2016. Technological Caregiving: Supporting Online Activity for Adults with Cognitive Impairments. (May 2016), 5311–5323.

[31] Piper, A.M., Cornejo, R., Hurwitz, L. and Unumb, C. 2016. Technological Caregiving: Supporting Online Activity for Adults with Cognitive Impairments. Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16 (Santa Clara, California, USA, 2016), 5311–5323.

[32] Rosson, M.B. and Carrol, J.M. 2009. Scenario-based design. Human-Computer Interaction: Development Process. CRC Press. 146–161.

[33] Smith, A. 2017. Americans and Cybersecurity. Pew Research Center: Internet, Science & Tech.

[34] The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry: 2019. https://citizenlab.ca/2019/06/the-predator-in-your-pocket-a-multidisciplinary-assessment-of-the-stalkerware-application-industry/. Accessed: 2019-12-24.

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

[36] Wan, L., Müller, C., Randall, D. and Wulf, V. 2016. Design of A GPS Monitoring System for Dementia Care and its Challenges in Academia-Industry Project. ACM Transactions on Computer-Human Interaction. 23, 5 (Oct. 2016), 31:1-31:36. DOI: https://doi.org/10.1145/2963095

[37] Wan, L., Müller, C., Wulf, V. and Randall, D.W. 2014. Addressing the subtleties in dementia care: pre-study & evaluation of a GPS monitoring system. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (Toronto, Ontario, Canada, Apr. 2014), 3987–3996.

[38] Wang, Y. 2017. The Third Wave?: Inclusive Privacy and Security. In Proceedings of the 2017 New Security Paradigms Workshop (2017), 122–130.

[39] Wisniewski, P., Ghosh, A.K., Xu, H., Rosson, M.B. and Carroll, J.M. 2017. Parental Control vs. Teen Self-Regulation: Is There a Middle Ground for Mobile Online Safety? Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing (New York, NY, USA, 2017), 51–69.

[40] Wolf, C.T. 2019. Explainability scenarios: towards scenario-based XAI design. Proceedings of the 24th International Conference on Intelligent User Interfaces (Marina del Ray, California, Mar. 2019), 252–257.

[41] Wu, M., Baecker, R. and Richards, B. 2005. Participatory design of an orientation aid for amnesics. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (Portland, Oregon, USA, Apr. 2005), 511–520.