"Citizens Too": Safety Setting Collaboration Among Older Adults with Memory Concerns

NORA MCDONALD and HELENA M. MENTIS, University of Maryland, Baltimore County

Designing technologies that support the cybersecurity of older adults with memory concerns involves wrestling with an uncomfortable paradox between surveillance and independence and the close collaboration of couples. This research captures the interactions between older adult couples where one or both have memory concerns—a primary feature of cognitive decline—as they make decisions on how to safeguard their online activities using a Safety Setting probe we designed, and over the course of several informal interviews and a diary study. Throughout, couples demonstrated a collaborative mentality to which we apply a frame of citizenship in opensource collaboration, specifically (a) *histories of participation*, (b) *lower barriers to participation, and* (c) *maintaining ongoing contribution.* In this metaphor of collaborative enterprise, one partner (or member of the couple) may be the service provider and the other may be the participant, but at varying moments, they may switch roles while still maintaining a collaborative focus on preserving shared assets and freedom on the internet. We conclude with a discussion of what this service provider-contributor mentality means for empowerment through citizenship, and implications for vulnerable populations' cybersecurity.

CCS Concepts: • **Human-centered computing** → *Human computer interaction (HCI)*; *Empirical studies in HCI*;

Additional Key Words and Phrases: Memory, cybersecurity, couples, older adults

ACM Reference format:
Nora McDonald and Helena M. Mentis. 2021. "Citizens Too": Safety Setting Collaboration Among Older Adults with Memory Concerns. *ACM Trans. Comput.-Hum. Interact.* 28, 5, Article 31 (August 2021), 32 pages.
https://doi.org/10.1145/3465217

1 INTRODUCTION

Older adults experiencing memory concerns, including fear of further decline in memory competence, and who might ultimately have a diagnosis of mild cognitive impairment (MCI), regularly confront the challenge of being safe online without loss of agency or autonomy to carry out the activities of daily life [41, 45]. While online activity is a critical component of well-being for this demographic, it also presents unique privacy risks because older individuals are increasingly targeted and thus, potentially more susceptible to internet harms, including scams perpetrated by others and their own risky behaviors [41]. There is an important challenge for human-computer interaction (HCI) scholars in thinking about these individuals not as patients, or potential patients, but rather, as citizens who require a certain type of cooperative care, with "power entitled to the

This work is supported by the National Science Foundation under Grant CNS-1714514.
Authors' addresses: N. McDonald and H. M. Mentis, University of Maryland, Baltimore County, 1000 Hilltop Circle, Baltimore, Maryland 21250, USA; emails: norakmcdonald@gmail.com, mentis@umbc.edu.

1073-0516/2021/08-ART31 $15.00
https://doi.org/10.1145/3465217

same life as everyone else" [2]. Yet with that power and agency might paradoxically come the price of mutual surveillance—of collaborative cooptation of surveillance. This is the micro–macro challenge of agency for those experiencing memory changes [2] in surveillance capitalism [61]. That said, opensource environments provide insight into how to negotiate these collaborative and empowering arrangements.

At the same time, it is important to consider the perceptions of security threats among those who share the challenge. While the responsibility of supporting safe online activities on social networks, email, banking and shopping sites often falls to caregivers [3, 33, 45], caregivers are not necessarily empowered, themselves, to offer the kind of support that would achieve what might be considered safe autonomy for their couples. A recent PEW report indicated that most Americans do not feel in control about the data collected about themselves [8]. The implication is that they are even less well-equipped to secure partner privacy online.

For couples—one or both of whom might have memory concerns—maintaining security is potentially a collaborative enterprise where they are trying to determine how to balance online safety and privacy and agency. Being safe online for couples with or without memory loss involves issues of deep trust and cooperation due to the very nature of partnership and the implications of shared online data or data linkages. It might test the strength of their sociotechnical relations since effective cooperation is needed to withstand or mitigate outside threats. But issues of agency in research further complicate this narrative, raising questions about how to define or measure agency (or its loss) and how to avoid implying to participants that the researcher is offering a technology solution that will, in fact, support them fully on an uncertain journey. For partnerships in which one or both have memory concerns, the stakes are higher, and the management of agency and safety becomes even more complex, as we consider agency *for whom* and safety *from what* in the context of highly interconnected identities.

This article reports on findings from our initial testing of the safety mechanism options with couples where one or both is experiencing "memory-related concerns," as well as a diary study designed to explore how couples perceive threats and what that might mean for their choice of Safety Setting. This research is part of a larger project exploring the challenges of *collaboratively* safeguarding cybersecurity for couples where one or both has memory concerns or loss and the need for more choice and flexibility in applying technological safeguards for couples [34, 38, 40, 41]. Prior to our most recent work studying Safety Setting scenarios [39], we developed a technology probe that charted the uneven and unpredictable process of selecting cybersecurity safeguards. In this article, we focus on the nature of the collaborative process of decision-making demonstrated through a framework of citizenship and open collaboration discovered in our technology probe study. We also introduce findings from a diary study we conducted to explore in depth how couples collaboratively deal with threats. Additional results from couples *choice* of Safety Settings from the technology probe study are detailed in [38].

Because deterioration in memory is a pervasive age-related experience and is not necessarily accompanied by a confirmed diagnosis of any kind (including MCI), our goal was to study people in partnerships who *perceive* memory loss, or have *concerns* about memory performance, rather than to study people with formally diagnosed memory loss.

HCI and computer-supported cooperative work (CSCW) have developed approaches like action research (AR) [22, 23, 60] to address issues of agency and vulnerability. More traditional ethnographers have also developed methods like the extended case method, which deploys reflexive observation study to mitigate the effects of power [11]. Understanding the implications of structures of power, and specifically their impact on vulnerable identities, requires sensitivity to normalized views about "safety"—a term which is, itself, gendered by its application to studies of vulnerable people [12]. Of course, there are limits to this insight when we are dealing with couples whose

memory concern is clearly more severe, but our study ultimately challenged us to consider: Is it really the case that one member of the couple will have to monitor the other or does our research impose those roles inappropriately, or too soon? (Our "setup," detailed in this article, was particularly critical for eliciting this thinking.) Can we build a technology that incorporates a more flexible and adaptive conception of cooperation and agency in relation to partnership and memory concern?

We are seeking to devise a technology built on users' own terms, without imposing an external view of whatever memory deficit (or perceived deficit) it is meant to help mitigate or requiring oversight to fall entirely on the shoulders of a partner. While the responsibility of supporting safe online activities on social networks, email, banking and shopping sites often falls to caregivers [3, 33, 45], they are not necessarily empowered, themselves, to offer the kind of support that would achieve what might be considered safe autonomy for their couples.

We introduced a Safety Setting probe whose intent is to provide technology choices that empower couples to enhance their security practices, and we used naturalistic observation to discover how they interacted and behaved in relation to the choices made available by the technology. Our approach involved having couples first engage in sociotechnical negotiations during a "setup" phase before engaging with our safety probe "study." We did not ask explicitly about memory concerns and challenges during the interviews but rather, observed how these couples negotiated everyday technical problems and made safety setting choices in this context, with the goal of learning specifically:

1. Do they talk about their future together in the context of memory concerns?
2. Do they establish criteria for their future self, which might lead them to alter their choices?
3. Do they engage coequally in talking about their selection?

We find that couples do talk about a future trajectory with memory concerns and about adjusting Safety Settings if "things change," but we also find that criteria for adjusting behavior on behalf of those future selves is, in most cases, vague, and often based on experiences borrowed from their observation of others (aging parent or relative) rather than drawn from the specifics of their evolving experiences. Being the focus of memory concern in a relationship does not necessarily lead someone to assume a more passive role in the relevant negotiations and decisions. Couples frequently engage coequally in discussions about settings, and, in fact, it is often the individual with (greater) memory concerns who is more likely to steer the technological setup and Safety Setting selection.

We found that couples' perceptions and mitigation strategies with regard to online safety in the context of memory concerns—which is a primary feature of cognitive change—involve cooperative effort, built on years, if not decades, of sociotechnical habits of living.

To explore agency and power, we build on notions of citizenship that have emerged in some of the literature on adult aging [2, 32]. We draw on the metaphor of the collaborative platform model to organize our findings, discovering that partner decisions tend to hinge on principles of collaborative environments: histories of participation, lower barriers to participation, and the need for sustained participation.

2 RELATED LITERATURE

2.1 "Memory Concern": Hidden, Uncertain, Undiagnosed

Although this research does not involve dementia patients, memory loss is a primary criterion for diagnosis of MCI and the most easily accessible proxy for MCI diagnosis in a study of this kind, which relies entirely on participant self-reports. Our system is being designed to support couples

through the experience of memory decline (or perceived memory decline) through a possible MCI diagnosis. Dementia may go undiagnosed for long periods, but these couples may still benefit from support for their memory, especially with a system that gradually adapts, as we will describe.

MCI is characterized as a decline in cognitive function that goes beyond normal aging, but which has not reached the clinical definition of dementia caused by Alzheimer's or other cognitive disorders. People with MCI can have problems not just with memory, but language, thinking, and judgment; and while they are more likely to develop Alzheimer's or dementias, some do not [42, 48, 58]. Although prevalence estimates for Alzheimer's vary considerably [48], recent estimates place prevalence at over five million people in the United States [17, 52]. Additionally, over 16 million Americans provide unpaid care for individuals with Alzheimer's or some other type of dementia [17]. MCI affects 14.9% of those 65 years and older, with incidence rising in each decade of life beyond 70. Not only are individuals with MCI at high risk for progression to dementia; their symptoms may require additional care from couples and other family members. This is especially true for people in earlier stages of cognitive decline, whose symptoms are milder and are likely to still be living in their home.

Whatever their formal diagnosis, individuals with MCI and/or memory concern may be uniquely susceptible to threats as their diminished cognitive abilities can leave them unable to discern or mitigate risk. At the same time, they may greatly benefit from access to internet technologies [31]. Many studies have looked at designs for people with dementia in the context of an advanced condition [55], but less have looked at the gradual (decade-long or more) journey to that point. Ultimately, responsibility for overseeing online interactions and protecting against scams will fall to whoever in the family is most proximal and best equipped to exert supervision or oversight [41, 45]. This role can be significant for family members and caregivers who may not be fully equipped to exercise it (based on their own sophistication or sightline) and who, regardless, must balance the desire to avoid placing family members (and themselves) at risk against the desire to avoid removing all autonomy. Although the online risks associated with cognitive decline are easy to imagine, few studies document the degree to which aging populations (and those with age-related memory loss) experience adverse consequences [27]. Identifying protective measures that are both empowering and practical presents a meaningful HCI challenge.

2.2 The Problem with Privacy Technology Built for Normative "Users"

Privacy theory has a long history of perspectives that present or assume normative constructs of the "user" [4]. Most of the technology we use in our everyday lives was designed with an individual user in mind. The design of that technology is predicated on a conception of the user as someone who (1) has discrete, well-defined personal boundaries that do not overlap with others, or which they can regulate [1]; (2) makes privacy decisions in a social vacuum or noncollaborative context; and (3) has agency over privacy choices and protections [57]. There are reasons to debate the validity of all three of these assumptions.

First, the identity boundaries around users of technology are both complex and permeable. There has never been a single self, even if technologies have, at times, enhanced the opportunities for self-exploration [9, 54]. Technology, by its nature, lifts the curtain on our multiple identities in a way that challenges the boundary regulation of public/private life and self [44]. All those boundaries, including temporal boundaries, literally collapse when users participate in technology [36]. Technology not only exposes (and merges) the multiplicity of selves we aim to compartmentalize and protect from view; it also puts others with whom we are connected at risk. The concept of the single technology user fails to do justice either to the complex subjectivity of the individual or to their complex linkages with the myriad identities of others [51]. Users are often members of social and economic units whose shared data, shared circumstances, and (frequently) shared

devices have implications for the privacy of others, and which put them at shared risk. Privacy violations experienced or permitted by one member of that unit can have profound implications for others.

2.3 Designing for Collaborative Citizenship

While technology offers a means for partners and/or caregivers to potentially extend support to those with memory impairment while living at home—for instance, by keeping tabs on their online activities—Mahoney et al. point out important ethical issues that arise from home monitoring [35]. Age and memory concern do not equate to ability, but the work of Mahoney et al. is instructive in its emphasis on the importance of respect and autonomy, *as well as* respect for family caregivers and relationships with people they assist. By calling attention to these relationships, these authors usefully highlight the way in which end-users also include family and patient collaborators.

In their study of collaboration among individuals with dementia and their caregivers, Hwang et al. [28] finds that equity in decision-making and power supported "collaborative appropriation" of technologies. While our study does not explore those relationships exactly, it does suggest that approaches that consider shared power to be integral to collaboration may be ideal—even if straining what might be practical.

Work by Piper et al. emphasizes the importance of designs that are invested in cooperative experiences while also raising cautions about the ethical and legal challenges of these designs [45]. For instance, the authors suggest that joint accounts might be part of a set of solutions for supporting technology dynamics among dyads but (citing Batchelor et al. [3]) also note that such solutions may present "ethical or legal challenges" [45]. Piper et al. also consider design of aware systems: "For example, a system could detect disclosure of sensitive information (e.g., passwords, credit cards) and hold the transaction for review by or feedback from the primary caregiver" [45]. They note the way in which online activities are worked through cooperatively, often *in situ*.

These sources share a focus on cooperative and collaborative work as a solution to navigating technology in the face of memory concerns, which require oversight to mitigate risk. Other literature points, similarly, to the importance of providing support, not just for those with memory concerns or MCI, but also for their couples and caregivers, and for the relationships needed to access and manage technology protections [34]. MCI management is, in this view, "a complex and cooperative social practice" [45], and one that "couples" do collaboratively [5, 25, 26]. Couples experiencing memory loss and facing dementia, we hypothesize, benefit from collaborative strategies for managing their lives and thus, their internet privacy and security.

We build on this work with a probe and a diary study that investigates further the nature of this partnership in a sociotechnical setting and with Safety Setting probe to elicit those conversations. Thus, while the shift toward a person-centered approach to thinking about cognitive decline has sensitized us to the importance of autonomy and respect [34], Bartlett and O'Connor make the case that citizenship (when thought of in broader sociological terms) may be an even more useful lens through which to consider the challenges of privacy and safety protection in this population. They view dementia (or similar declines in cognitive function) as a problem requiring social change and consideration of power [2]—rather than aging as a "problem" [56]. They argue that personhood (the antecedent of person-centered design [18]) does not necessarily promote a sense of agency, nor does it necessarily encourage sensitivity to the concept of diminished cognitive capacity as diminished power [2].

Lazar et al. pick up on this notion of citizenship in considering how people with dementia are challenged in the exercise of full participation in society [32]. One way that the concept of citizenship is useful is that it allows us to imagine everyone as equal couples and to consider the need to support not merely those with cognitive changes, but also the couples and caregivers

whose participation is being enlisted [34]. Indeed, memory concern is "a complex and cooperative social practice" [45] that couples may do collaboratively [5, 25, 26] and which may also involve children and other family members. Later in this article we consider how attempts to restore full citizenship to people experiencing cognitive loss might benefit from a conception of power restoration as the product of a collaborative universe where user participation is understood to be limited or constrained, and service providers must accommodate it by actively lowering barriers to participation.

Bartlett and O'Connor make the case for a sociological view of citizenship that considers power, agency, and structure [2]. They caution that citizenship, without consideration for sociological ideas, could, for instance, overstate or misapply notions of agency, which are linked to independent cognition. Perhaps a weakness of citizenship is that it can imply privileged membership and thus has the potential for exclusion. Citizenship also places priority on community and order, sometimes at the expense of the marginalized individual. If we imagine a partnership or family that is struggling with cognitive changes of one of its members, the tendency may be to have that person conform. At the same time, there is opportunity for the community to change, to consider power, agency, and structures as Bartlett and O'Conner suggest. This could mean evolving the way that they think about internet use as something that requires more cooperative practice. Accordingly, we consider that the requirements for this cooperative membership introduce risk of surveillance. It is important to remember that analogs for the dynamics of surveillance among vulnerable users do exist and are a real danger for those engaged in using this type of technology—for instance, children (e.g., [30, 59]) and in the context of intimate partner violence and surveillance (IPS/IPV) (e.g., [20, 53]). Indeed, in our study, couples mention that the more restrictive aspects of this technology would be best suited for children or those with more severe cognitive disabilities, and thus could present a threat to their partnership.

The tradeoffs between surveillance and safety are nevertheless usefully prompted by citizenship and concepts of social awareness and accountability, which characterize collaborative environments. We discuss the importance of collaborative infrastructures in the next section.

2.4 Conceptual Framing Based on Open Collaboration

As we analyzed our data, we started to gain conceptual clarity by connecting our results to notions of shared infrastructures and collaborative models of participation. For this reason, we turned to the concept of open collaboration models, which, according to Forte and Lampe, share in common "an online environment that (a) supports the collective production of an artifact (b) through a technologically mediated collaboration platform (c) that presents a low barrier to entry and exit and (d) supports the emergence of persistent but malleable social structures" [19]. The open collaboration model is a useful metaphor because open collaboration models rely on the visibility of users' participation and on policies that support participants' roles as trusted citizens of a community built on shared infrastructure. These models achieve efficacy by lowering barriers [10] and insisting on social translucency [37]—attributes that make them vulnerable to infiltration and disruption by bad actors. There is a rich literature that speaks to how these open collaboration communities are tasked with mitigating such threats [21]. Social translucence works in knowledge communities because it is concerned with mechanisms that do not just identify the need to see what others are doing, but also the social value of visibility in creating awareness and accountability. As Erickson and Kellogg point out, putting glass in a door ensures the safety of those passing through by introducing awareness of who is on the other end and, importantly, accountability because one actor can see the other seeing them on the other side [16].

Cooperative infrastructures are sites of social relations, power, and politics, "a fundamentally relational concept, becoming real infrastructure in relation to organized practices" [50]. As such,

we attempt a sort of "infrastructural inversion" [50] by thinking about the properties of the Safety Settings and conversations as part of relationship articulation. In taking care to avoid "caregiver" tropes, we defer to the sociotechnical practice that preexisted any Safety Settings.

We find that couples are drawn to the system because of the possibility of collaborating on their cybersecurity—not on watching over the other. It gave couples the kind of role they wanted and also respected the mutual autonomy of each other and their relationship, as we will describe in the findings.

The need to produce a system that adapts with partners' memory circumstances might put greater emphasis on the need to build a collaborative system, but couples we have studied thus far have indicated that maintaining awareness, even while one or both are declining is critical; partnership is critical.

2.5 Enacting Disruption or Reflexivity in Design Work with Technology

Although memory concern might ultimately lead to the loss of autonomy for one partner, we suspect that couples will maintain preexisting sociotechnical roles for as long as they are able, rather than submit readily to a patient/caregiver model. In considering how historic roles might persist, even in the face of memory concerns that might put such roles and relationships to the challenge, we borrow from the concept of the reflexive turn [47]. The reflexive turn in ethnography attempts to redress issues of power and positionality in applying observational or interventional methodologies [13]. In this case, it inspired us to take an approach that actively investigated responsibility for "solving" sociotechnical problems, rather than simply imposing solutions. In our work, we consider not just the broader context of agency and shared memory concern, but also, the shared sociotechnical world these couples have historically inhabited together as a couple. Years of negotiating sociotechnical roles, habits, and informal policies in a collaborative landscape of domestic partnership have, no doubt, shaped partner approaches to managing memory concern.

Our analysis is partly directed at making sense of participants' sociotechnical space, and how they negotiated technology as partners during a "setup" prior to our formal "study." Our encounters with participants took place over days, and culminated in several-hour sessions, less than an hour of which involved engagement with the actual Safety Settings probe. Much of the interaction and observation centered on the process through which they reached that point of engagement—a "journey" that offered a unique sightline for the researchers. Burawoy writes, "[t]he reflexive perspective embraces participation as intervention precisely because it distorts and disturbs. A social order reveals itself in the way it responds to pressure. Even the most passive observer produces ripples worthy of examination, while the activist who seeks to transform the world can learn much from its obduracy" [11]. Similarly, ethnographic work in the design space provides answers to design questions on their own terms by staging "encounters" with design that leave open the possibility to new questions and reflections through a reframing of the context [14, 15]. We, too, drew heavily in this research on the notion of disruption or intervention by requiring couples to negotiate the preparatory steps in the teleconferencing system we used that were needed to engage with the probe, exposing sociotechnical relationships that would not otherwise have been evident [11, 46].

3 METHODS

3.1 Prior Research and Design

During the first two phases of this study, we conducted qualitative interviews and observational studies with caregiver/recipient dyads (spousal couples) where one was experiencing cognitive changes to understand how caregiver and recipients currently discuss and adjudicate online access

and safeguard options [34, 40, 41]. From these interviews we learned that while some dyads display little proactivity in this regard, some do take very seriously the need to plan ahead and discuss issues of access with each other. We also learned about the types of online safety management procedures they employ using the technology and settings (or preferences) currently available to them. While Couples are sometimes planning ahead for a time when the one with MCI is unable to engage online as before, we found that concrete discussions around cybersecurity and access are at best abstract, such that recognition of those moments was delayed or challenging to manage. Couples were often caught off-guard when the time finally came and sometimes prone to take measures that disempowered MCI individuals altogether [41]. This is yet another reason why we chose to focus our intervention on couples who have or perceive they have memory concerns, rather than a concrete diagnosis.

We designed a probe that would build on these findings, with the goal of empowering couples confronting memory concerns by offering them a series of Safety Setting choices. The probe was implemented to elicit more detailed insights grounded in actual settings to understand better how decisions about Safety Settings might be handled cooperatively between couples, especially in the early stages giving them time to adjust—since as we pointed out sudden measures with later stage couples can prove disempowering and harmful. It was critical to explore with individuals experiencing memory loss (as opposed to confirmed MCI) to learn the full range of use of this system, from (current) suspected memory loss to (future) potential MCI. The mock-up provides safeguard features the couples can select together, revealing where they ultimately situate themselves along the continuum, as well as offering insight into how choices are negotiated.

McDonald et al. describes the approaches for safeguarding individuals as residing along a continuum between complete oversight by the caregiver and no intervention at all [38]. Explicit attempts to avoid disempowering these memory-challenged or concerned individuals required couples to find a middle ground that accounted for dynamism in the cognitive status of the memory-challenged individual, and also preserved some semblance of historic normalcy in the relationship. This required significant work on the part of the caretaking partner, but it was clearly deemed preferable to a set of binary, all-or-nothing, oversight options that deprived couples of flexibility [38]. Couples are eager for a nuanced set of options that help them navigate between abdication and removal of all power, while also accommodating their historic relationship dynamics, experiences, and changing proficiency levels.

This article reports on the collaborative interactions of couples while using a technology probe as well as over the course of a diary study in which couples report on threats they encounter in their email inbox or elsewhere on the internet. It uses a novel framework of citizenship and open-source collaboration to illustrate the benefits of thinking about this process as part of collaborative enterprise that honors their relationship and ensures their mutual dignity.

3.2 Study Design and Procedures

3.2.1 The "Setup". The structure of the study design was layered in the sense that its ostensible objective—the stated goal of observing couples in the act of using an experimental technology probe was the impetus for enrolling them in a study whose observational focus was both the setup process and the probe. At least as much time was spent in naturalistic observation of partner interactions as they worked to overcome the spontaneous hurdles they encountered in the process of engagement with the GoToMeeting platform.

During this "setup" phase which included securing signed consent, the researchers interacted with each pair in a variety of impromptu ways, for instance: connecting through Facetime, helping participants with the printing and sending of consent forms, resending an email with the meeting invite, or trouble-shooting device challenges to optimize remote access. By taking no special

preemptive steps to avoid these technology obstacles, we allowed them to arise, providing opportunities for the researchers to observe spontaneous collaboration as challenges arose. These "setup" activities became a thick, interpretative space in which we learned how couples negotiated everyday technological tasks and coped with surrounding uncertainty. The process by which tasks were managed revealed the sociotechnical order of the household—i.e., the way members of the dyad related to technology; what unwritten "policies" and practices there might be; and with whom among the couples responsibility for technology leadership might reside. Observation and interpretation of these tasks provided important context for understanding the dynamics of their sociotechnical relationship as a couple. They also highlighted the fact that memory concerns and technology leadership can coexist in the same individual, adding one more element of complexity (or adversity) to the challenges these couples confront when the technology leader of the pair experiences some loss of efficacy.

3.2.2 The Safety Setting Technology Probe Study. In the probe study, we presented the technology probe that gave couples an opportunity to select Safety Setting safety mechanisms for situations in which they use technology—couples could select any or all of the categories to set their Safety Settings. We asked them to share aloud their thought process and speak freely with their partner as they decided what settings were most appropriate.

While couples were told they would be given remote access to the researcher's screen so they could click on the chosen radio button, only two couples were able to accomplish this (either for personal, technical, or device-related reasons). In all other instances, the researcher instructed them to simply verbally indicate what settings they chose together.

Each technology probe session was followed by a semistructured interview designed to explore the perceived usefulness of settings, how couples might elevate privacy concerns, and how they might evolve over time if memory concerns worsened.

3.2.3 Technology Probe Design. We presented a technology probe that gave couples an opportunity to select safety mechanisms for situations in which they use technology, including email, Facebook, online banking or money transfer, online shopping, password management, and online browsing. Couples were asked to make Safety Setting selections through a Safety Settings html page. The ultimate goal is to develop a browser plugin application that map to these settings choices and engage couples as they perform online activities in a way that safeguards them on terms they find both manageable and easily understood.

As a "low-fi technology application" our technology probe provided information about potential use and served as inspiration for design [6]. It was not an iterative design step. Rather it aimed to subvert traditional HCI design methods by opening up our thinking about the potential design itself. Borrowing more from traditional notions of cultural probes and the notion of empathic engagement, we did not (as noted in the next section) ask couples to identify who was "suffering" or who had "memory concerns" nor even talking about memory at all.

Couples first selected the online application/situation categories available in the probe that they said they use; they could select as many as they wanted from Table 1, Column 1. For example, couples were asked if they used/did Email, Facebook, Online, Online Banking, Online Shopping, Password Management, and Online Browsing. Then they were asked for which of those applications/situations would they want to have some type of settings that would help them manage internet security threats. For each application/situation couples chose, they were given the same set of corresponding actions that the Safety Settings would be used for (shown in Table 1, Column 2). For example, if a couple said they used Email, they would select Safety Settings for the following actions: "clicking on a link in an email message" and "opening attachments in an email message." For *each* of these actions (Table 1, Column 2) couples were asked to set Safety Settings.

Table 1. Online Context and Actions one Could Perform that Entail Safety/Security Risk

Application/Situation Category	Online Actions Taken by a Partner
Email	Clicking on a link in an email message. Opening attachments in an email message.
Facebook	Liking a Facebook post. Commenting on a Facebook post. Accepting/rejecting a Facebook friend request.
Online banking	Viewing bank/financial account online. Transferring money online.
Online shopping	Visiting a site to purchase a product. Purchasing a product online.
Password management	Setting/changing password to an online site. Setting/changing password to computer.
Online browsing	Searching for information on the internet. Clicking on a link to download a file off the internet.

There were several choices for Safety Settings: "not interfere," "record for partner to see later," "notify partner," "partner review before continuing," "review prior to posting" (Facebook only), and "deactivate/not allow." Figure 2 shows a screenshot of the Safety Settings as they were displayed to participants. This spectrum we have described ranges from "no interference"—i.e., the Safety System would take no action when the person with cognitive challenges performed the action—to what we deem "full interference"—i.e., the Safety System ensures that the action cannot be completed. What is important to note is that between these two ends of the spectrum were three to four additional "levels" to choose from, which provided flexibility beyond what couples feel they can currently do. As the choices moved from no interference to full interference, the choices generally added more security, with a corresponding reduction in autonomy and privacy. We observed participants discuss these options.

In summary, for each application/situation category in Table 1, Column 1 couples specified whether they would want protection form threats; they were then given the option of selecting Safety Settings (i.e., "not interfere," "record for partner to see later," "notify partner," "partner review before continuing," "review prior to posting" (Facebook only), and "deactivate/not allow.") for each of the corresponding two to three actions listed in Table 1, Column 2.

We introduced the probe using two screens, one which presented the application/situation and one that presented the actions and Safety Settings. Figure 1 shows the application/situation screen. Figure 2 shows a screenshot of the actions and Safety Settings as they were displayed to participants (for the email). We did not present scenarios to the couples in this research as we did later in [39]. We asked couples to reflect on what they currently do, for what applications they would want Safety Settings, and what those Safety Settings should be from the list of options. Couples were asked to walk through the system using remote access given through GoToMeeting or, in instances where they were using their phone or iPad and or for other technical reasons could not access the remote access, by telling the investigator what to select. We listened to them talk about their own scenarios for each application/situation, action, and Safety Setting they selected and also engaged with them in follow-up discussion.

Part of the reason why we call this a technology probe is that we use the Safety Settings across multiple studies to gauge feelings about restricting behavior and to engage couples in participatory design. We used the probe to engage participants after the diary study in discussion of whether, given their experience, their original Safety Settings selections might change. We also later used it to structure a scenario study [39].

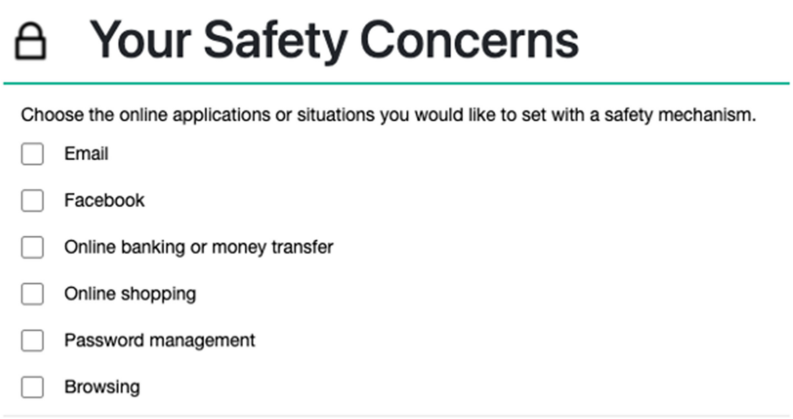

Fig. 1. Application/situation options display screenshot.

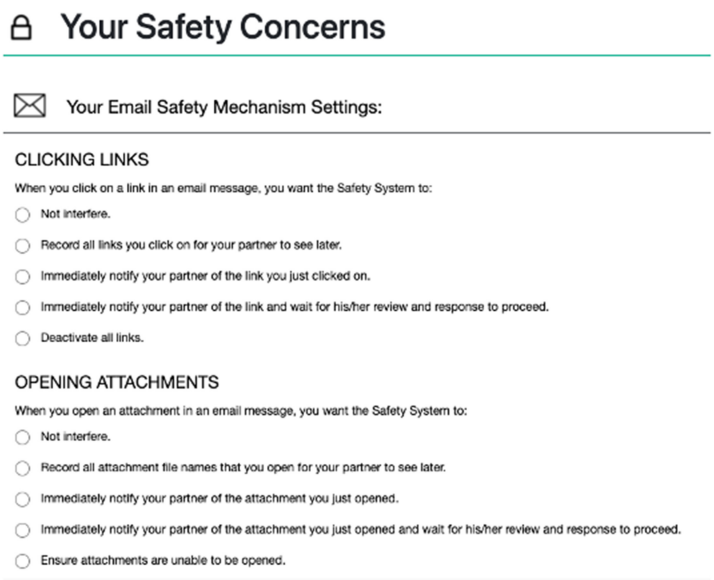

Fig. 2. Safety setting options display screenshot (email).

3.2.4 Diary Study. In our diary study, we provided couples with an online diary using Google Forms and asked them to report on privacy and security events as closely to the event as possible over the course of a month. During out orientation for the study, we provided couples with a separate description of what cybersecurity events *could be*, including a list of possible events. We also told them to make entries for any occurrence that made them feel uncomfortable or worried about their privacy and security online. Specifically, we described a cybersecurity event as *possibly*:

- An attempted breach to data security or privacy, such as getting a suspicious link, or ending up on a site that you thought might be dangerous.
- Things you did not intend to do, for example posting to Facebook or purchasing something you/your partner did not intend to or later regretted, and so on.

Table 2. List of Possible Cybersecurity Events Provided to Participants in Orientation and in the Google Form

Here is a list of specific things that we consider to be events. *But we have surely not covered them all.* Anything else that made you worried about your cybersecurity that we have not thought of *we also want you to include as an entry.*
Received/clicked on an email attachment that I/my partner suspect or know was phishing
Liked a link on Facebook that I /my partner suspect or know was malicious or embarrassing
Posted something on Facebook that I/my partner should not have or regretted
Went to banking site that I/my partner suspect or know was not the real site (e.g., spoofed site)
Entered sensitive data into a banking site that I/my partner suspect or know was not the real site (e.g., spoofed site)
Transferred money to someone I/my partner should not have
Went to shopping site that I/my partner suspect or know was not the real site (e.g., spoofed site)
Entered sensitive data into a shopping site that I/my partner suspect or know was not the real site (e.g., spoofed site)
Made a purchase on a shopping site that I/my partner should not have or regretted
Received notification of a password breach I/my partner suspect or know was the result of someone else changing my/our password
Could not get into a site with my/our password and had to change it
Was browsing and I/my partner got lost and did not know how to find the site again
Downloaded a file that I/my partner should not have
Other, please specify

We included a list of cyberthreats but told participants that the list was not exhaustive (Table 2). This list was also provided in the Google Form, where, for each event they reported, we asked couples to choose an item from the list or specify something else. We had them describe the event and how it made them feel. We asked for ratings of their concern. We also asked what steps they took during and after the event (e.g., Did they contact the business or sender? Did they report the email or website? Did they research the link, sender, or business?); what they said to their partner about it; and whether and how it would change their online behavior). (See Appendix for diary study Google Form given to participants.)

During the study participants sometimes texted or emailed photos of events, so we added a place in the Google Form for them to upload audio, video, or images. While for all three couples, only one member of a couple made the entries into the Google Form, they also described events that had happened to their partner.

Over the month-long diary study, we followed up with couples every Monday morning to remind them to contribute only if we had not seen an entry from them in several days. We also interacted with them on several occasions when they texted or emailed about events that they wanted to ensure were relevant, or to let us know if they were taking a few days off because they would be away from their computer.

Following the month-long diary study, we conducted a 30–60 minutes interview with couples where we asked them to reflect on themes from their cybersecurity diary (most of which we supplied from reading their entries) and also asked about specific events to learn more or gain clarification about what happened. Before we had these meetings with couples, two members of the research team open coded every entry from the diary study. We then met to discuss and apply the themes reported in our findings. These themes were at the center of our discussion with couples.

3.3 Participants

Participants were initially recruited from a market research panel and, in one case, a continuing care facility. We studied a total of 14 participants (7 dyads) for the technology probe and 6 participants (3 dyads) for our diary study. For a couple to qualify, both couples had to be 65 and older; one or both had to have memory-related concerns (it was not relevant for us to document which in the screening process); and one or both had to have security concerns online.

The market research panel from which we recruited our participants maintains a panel of individuals and caregivers suffering from conditions ranging from asthma to various types of cancer. These are individuals who have opted in to be contacted for research. We screened 867 participants who were 65 and over living in New Jersey, Pennsylvania, Delaware, and Maryland (assuming we wanted the flexibility to research in person) and found only six couples with memory and cybersecurity concerns who were willing to participate for $37—significantly less than they typically receive for this panel.

For our diary study, we sent emails to couples who participated in the probe study with a request to participate in follow-up research. Three couples agreed to participate. Couples were given a $150 honorarium with the expectation that the study could potentially involve several hours of their time throughout the month and including a 15–30 minutes orientation interview and 30–60 minutes closing interview.

Because of the sensitivity of this subject matter, we did not gather specific demographic information. Couples were mixed race, retired or semiretired, between 65 and 80, and living independently. They had demonstrated knowledge and proficiency with more advanced security concepts—e.g., an understanding of how phishing works (including through attachments) and how to detect it through technical means; and an understanding of the principles of data capitalism (how, for instance their data is sold and repurposed for algorithms). From later research with these couples, we learned more about their proficiency with internet and financial security. For instance, one couple was on high alert about purchases their partner made that seemed to be risky and was monitoring their credit card statements and email. Another decided to implement two-factor authentication as well as browser shortcuts to increase awareness and circumvent threats to financial accounts. They all had a sense of how their internet (and even offline) activities result in unwanted communications through email. While all are comfortable with computing devices, video conferencing technology proved challenging in our initial interviews; it may be because GoToMeeting is relatively not easy to use.

We chose memory concern for this study (as opposed to MCI) because we wanted to learn about how couples adopt this technology into their lives early on and how they adjust settings over time, with the plan to follow these individuals over the long-term. We took an approach to research that was collaborative and met participants on their own terms. We do not ask for a specific diagnosis or invite couples to assume labels or roles. Specifically, we used self-reported memory concern in determining eligibility, but it ultimately became apparent in the interviews that both couples in all dyads had some memory insecurity, or anxiety associated with aging or disease. Specifically, we asked respondents if they or their partner identified as having: "experience[ed] problems remembering things such as where you left your keys or peoples' names?" We believe this made for more honest and natural interactions. For instance, one couple repeatedly claimed that they are *both* experiencing memory loss, and believe that this is, in part, a way of showing compassion for the other partner—so they do not feel singled out. We ultimately learned who is experiencing more memory change (and from what), but we allowed that information to come out during the course of our relationship with these couples.

Focusing on couples in a study of a "surveillance" technology invites questions about agency and the potential for the arrangement to suppress concerns about it. We did not *formally* interview participants individually because our study was designed to uncover a collaborative process and outcome. But we are very sensitive to the potential for dark uses of these kinds of technology and did informally interview individual members of the dyad on several occasions—including those who had memory concerns.

3.4 Data Collection

The setup, observations, and interviews of the *Safety Settings technology probe sessions* were captured through notes, on video, audio, and screen capture with participants' permission and IRB approval. In total, sessions lasted anywhere from 1.5 to 3 hours, depending on how much socializing, technology, and logistical maneuver were involved. The technology probe portion, in which setting choices were made and rationales for selection were discussed, lasted for roughly 20 minutes, but additional discussion about technology use and the future of memory loss with a system that provided these Safety Settings lasted roughly 1.5 to 2 hours. Thus, while the time spent interacting with the probe may have been short, the discussions the study elicited extended over an hour. The probe served its purpose of exploring potential use and providing inspiration for design. All interviews were transcribed and safety selections, recorded. Consent forms were completed before or during the study.

We spent additional hours with participants conversing over email, phone, Facetime, and WebEx, about security and memory loss and perceive threats, all of which touched on the probe. We also conducted a diary study over phone, email, text, and Google Forms (described in more detail below). Our relationship with participants was ongoing.

For our *diary study*, we collected data using online Google Forms and follow-up interviews, which we audio/video recorded. We collected a total of 54 diary entries over a one-month period. Follow-up interviews lasted 30 to 60 minutes and were captured using video/audio recording. During those interviews, we asked couples to tell us about important issues that came up and how they dealt with them and we presented and probed themes we had coded from their diaries (detailed in our data analysis section). At the end, we had them review their Safety Settings from the previous probe study and recorded any changes as well as the reasons. The quantitative results from the diary and review of Safety Setting changes (detailed in our procedure) are not explicitly reported in our findings but were useful to direct our discussion and analysis of themes.

3.5 Data Analysis

3.5.1 Technology Probe Study. Videos and audio of our probe study were watched and transcribed. We used a phenomenological [49] thematic approach [7], organizing and grouping our findings into themes related to collaborative environments but also privileging respondents interpretations of their experiences. The primary researcher and first author directed the analysis and meet regularly with the other author to discuss interpretations. We focused on the way in which couples made decisions around the Safety Settings page as a collaborative unit, finally grouping our findings into themes that related to features of participation and sustaining participation.

The activities we introduced included both the technical setup of the meeting and selection and negotiation of Safety Settings presented in our Safety Setting technology probe. We used spontaneous "disruption" in the setup and the associated findings to create context for our interpretation of the probe setting decision process and follow-up interviews. This was particularly important in our findings about decision-making because we were able to derive insight on sociotechnical roles by observing couples during the setup period. This notion of open collaboration platforms is an apt metaphor here because it represents an environment in which participants function as citizens

in a community of contributors, and contribution is actively nurtured for the benefit of both the contributors and the community served by platform. In our findings, we mostly cite quotations from the discussions around settings choice, but the observation of couples' sociotechnical habits gleaned from the setup (which when cited where recorded with their permission) was critical to our analysis. For example, when we say in the findings "the CP2 partner with more memory concerns (CP2-1) led the technology setup and walkthrough." This "setup" analysis was performed after a consent was signed and recording agreed upon.

3.5.2 Diary Study. We open coded every entry from the diary study using a combination of open-ends and quantitative results provided in a Google Form questionnaire (see Appendix for Google Form). We also tallied results to get visualizations of what were the most important threats. We then met to discuss and apply the themes reported in our findings and that were used to frame our follow-up interviews. Audio of our follow-up interviews were transcribed. The researcher who conducted the interviews also took detailed notes, including changes to Safety Settings. Only one couple felt that they were going to change their Safety Settings based on the incidents they reported. Given our small sample, we do not report these or other quantitative Google Form survey results.

4 FINDINGS: THE "SETUP"

We present findings from our setup to illustrate the way in which couples' roles are dynamic and collaborative. It was precisely in these moments of technological challenges that we learned how knowledge of someone with memory concerns may have trumped that of their partner and led to an unpredictable and uneven power dynamics. Exploring these moments became the impetus for our thinking about how power, agency, and structure interact and led us to consider what membership in a partnership or citizenship might look like.

We found during our setup that, in some cases, the partner with more advanced memory loss initially led the technical setup. This might have occurred because the partner with more memory loss was more technologically savvy. It also reflects the way in which relationship dynamics override memory issues and technology decisions. A typical exchange in the setup was as follows:

> Interviewer: So you should be able to see my screen. Do you see a turquoise screen?
> CP1-1: No.
> CP1-2: No.
> CP1-2: Oh there she is!
> CP1-1: There you are!
> CP1-2: Oh no. That's not it. That's a man.
> CP1-1: What does that say right there?
> CP1-2: It says, "quarterly report sales." So all we see is "connect using a headset or mic" and then …
> Interviewer: Oh, I'm sorry. So, so, so, select save.
> CP1-1: Alright, I'm saving.
> CP1-2: Yeah, don't touch the screen.
> CP1-1: I didn't touch. I just pointed. This says, "choose your mic." "Input and output." Okay and then there's the camera.
> CP1-2: There you are. Yayyyy!
> CP1-1: That's me.
> CP1-2: Yeah?
> CP1-1: But where is she?
> CP1-2: Can you see us?

This went on for some time until we learned that the remote access would not work for their technologies. There are several reasons why these types of exchanges are valuable. For one, it is virtually impossible to know which participant is the one who has more memory issues, and this influenced how we engaged with respondents. Second these sessions became the thick preamble and lens for interpretation in which participants seemed to achieve full participation, and through the messy dynamic of technology challenge agency seemed to be regained. These exchanges would help to reframe their technical roles and thus help the researcher to view memory loss concern as a shared object that went back and forth between couples (similar to their technical turns) whose roles in the process where not static patient and caregiver but units dealing with memory loss and uncertainty on their terms. In that way, these interactions also revealed technical dynamics and areas of expertise that supersede memory loss.

The following excerpt shows how the researcher is merely a bystander in technical setup mess. What you cannot read is the sound of the feedback that is occurring because both speakers appear to be on FaceTime and GoToMeeting, and then the couple triumphs. The technical win for the couple places them in the position of agency for the interview and like the previous exchange reveals a collaborative dynamic:

> Interviewer: Can you guys hear me?
> [Calling them back on FaceTime]
> Interviewer: [Feedback sound] Sorrrrry, I need you guys to unmute the GoToMeeting. So that we can talk through there.
> CP2-2: I believe he's unmuted. But he's looking at. [Conversation between couple is muffled.] He's using the volume on his iPad. Is there a, um …
> CP2-1: Here we are.
> Interviewer: No. There's an, um…
> CP2-2: He's got it.
> Interviewer: Let me just see. You're not unmuted. You're still muted on there. So, there's an, um…
> CP2-2: This is not going to work with you having it on there.
> Interviewer: At the bottom of your screen, you should see a mic icon, a camera icon and they're both green.
> CP2-1: Yes.
> Interviewer: Or well, they'd be grey.
> CP2-2: My husband would like me to hang up. So, I'm going to do that.
> CP2-1: I'm on with you here.
> Interviewer: Your mic is not working.
> CP2-1: Let's see. There, is that better?
> Interviewer: Yes. Perfect! Now we can hang up.
> CP2-2: Okay.
> CP2-1: Okay.

Note that in this exchange the partner wants to disconnect before establishing audio on the meeting application. The partner is perhaps frustrated with this (describing that she is taking orders when she says she will disconnect) but nevertheless gives in. It is only because the researchers says they cannot hear them through the remote application that they rethink this strategy and stay on, only to triumph almost immediately after.

These setup sessions approach something more naturalistic because of these technological binds provoked by the setup. The technical challenges (repeatedly getting messages to allow audio and video access) were foreseeable, but the twists and turns were not. Some of them might have had

to do with use of iPads or assistive technology already on their computer, but it was impossible to know without being there. That opacity actually served a certain ethnomethodological end because it "reframed the contexts and questions of design" [14] by insisting that the roles that we might impose of patient and caregiver were upended and replaced with the more natural relationships to technology that exist. Consider if we had simply presented couples with a screen accommodating all the technical challenges and idiosyncrasies revealed here (in these meeting set ups) and elsewhere, would they have assumed more the roles that we had laid out for them? Would the person with more memory concerns have dominated the discussions as they did? That is, we entered the space on their terms through an unrelated technology and that upended the terms of our research. The designer/researcher has virtually no agency by the time we arrive at the mock-up sessions; the couples though emerge somewhat triumphant having managed to initiate the study with the technology they have.

5 FINDINGS

Our findings concerning couples' discussions around their options for continual online safety in the face of cognitive impairment with our technology probe are organized around three basic concepts drawn from principles of governance in collaborative platforms:

(1) *Logging and creating histories of participation*: We find that couples' concern about progression of memory loss leads them to select logs because they like the prospect that both they and their couples would have immediate access to their history.
(2) *Lower barriers to participation:* Couples are determined to ensure that settings accommodate levels of mutual respect and autonomy that allow both couples to participate uninhibited, or with only modest oversite, so that they can adjust security settings on their own terms.
(3) *Maintaining ongoing contribution*: Couples engage collaboratively in discussions about settings and place a high priority in maintaining participation.

5.1 Logging and Creating Histories of Participation

Couples frequently rehearsed what could happen if one *or both* of them made a memory-related mistake of any sort for any reason. They considered spontaneously that these mistakes would require logs or audits to allow their couples to see what had been done. Couples tended to gravitate toward the option to log or record their activities for later, which gives them, or their partner, access to their histories (that is, couples often discussed mutual access to these logs). Couples almost never expressed concerns about any downside associated with knowing what the other does from these logs, or the privacy violation such record might produce. Though frequently speaking in terms of memory concern or loss, they seemed equally interested in securing a record that would help to document and organize shared online behaviors. In this way, they are looking for a kind of collaborative platform; having access to your history of participation [37] is seen as valuable to a privacy/security partnership.

To illustrate the point, CP2-2 claims to want access to their partner's records in case of (further) memory loss, noting that the organization is opaque, while CP2-1 would find utility in a history of what has been done, regardless. Both appreciate the idea of having access to records regardless of whom loses their memory more ("should my husband and I lose our memory more") as a form of self-surveillance ("see what I've done" (CP2-1)) and also a form of surveillance ("know what he's on" (CP2-2)). From our setup, we know what member of CP2 has been experiencing more memory issues, but that does not mean that discussions about settings are focused on them. Indeed, the

member of the couple with more memory loss is the one who seems to be more technical in their role:

> CP2-2: Well, should my husband and I lose our memory more, I think he understands most of my things, but I find whatever he does extremely complicated. We are not organized in the same way and to me he's all over the place. So, I would want a fixed place to know what he's on, what he needs to know, or what I need to know. It needs to be straightforward, not 14 different paths to get there.
> CP2-1: I just want a history of what I've done. I'll remember the logic used to why I went certain ways or take a different path. As long as I can see what I've done.
> CP2-2: But his logic isn't the way I think logically.
> CP2-1: Right.
> Interviewer: And you're associating that with wanting more rigid settings?
> CP2-2: Rigid. No, but the detail. I would like more information than less.
> CP2-1: And I'd like the detail clear and precise, so I don't have to try five different pathways until I get to the one I need.

In this exchange, the researcher is referring to "more rigid settings" which refers to those that would require the partner be immediately notified of a link that has been clicked on or their review, and so on. CP-2 wants information about what they and the other does, in case they need to retrieve their history. They do not see it as exerting more/less control so much as a necessity of maintaining the awareness to preserve privacy and security. When CP2-1 says "I don't have to try five different pathways" it is to suggest that should the other partner not be available or lose their memory, they have the security of a record of what has been done. CP2-2 likes it to be able to recall what they did.

Similarly, CP3-1 emphasizes the utility of logs to grant access to their own participation. Indeed, later CP3-2 emphasizes the utility of having links recorded for his own ability to retrace his steps:

> CP3-2: Yeah, I'd like to "record all the links I click on for our partner to see later." In other words, I have a log to refresh my memory because that's what I need.

Histories of participation are empowering. For example, the very idea of accessing these logs, and thus having agency over memory, satisfied CP3-2 who feels they would "need" the ability to "refresh [their] memory." In this case, the partner with a greater degree of memory concern is more inclined to take over (or resume) a technology leadership role, rousing them both to mutual agreement with the excitement of finding a setting they believe suits them as a couple. Yet, CP3-1 also feels that having the ability to record links will help them remember what they have done online because they cannot always "keep track" of this information:

> CP3-1 Just a log. I'd like to record all sites where you can enter your credit card number for your spouse or partner to see later. And the next one record old purchase amounts for your partner to see later. I'd like the second one, record all usernames and passwords for later because I'm having trouble keeping track of that now.

These conversations resonate with the spirit of collaborative models in which records of participant histories are kept for the sake of all in the community, both to reward and to regulate participation, even if, as CP3 indicates, these logs may be put to different use by each of the couples. This is, indeed, similar to the kind of transparency that supports participation in open collaborative communities, where histories are used by participants to retain access to their own participation

and/or to secure access to the participation history of others, in order both to accomplish tasks and to contextualize participation.

Even while some couples tacitly acknowledge log-related privacy issues, logs are, indeed, seen as a liberating feature for both participants. The desire for a "record," "log" or "audit" is helpful because reviewing the links they have clicked on (i.e., which is what the record feature would do) is something both couples might currently do—either to facilitate oversight (safety) or to retrace steps if either partner forgets something (practice or participation). CP4 is reluctant to infringe on the other's activities, saying it is not "realistic" and so chooses to record rather than intervene:

> CP4-1: No. Not at this stage. If we were having more problems, maybe. But not right at the stage how we are because we don't want to have to wait if I ordered something or anything like that.
> Interviewer: Okay.
> CP4-1: To talk to him because it's just not really realistic right now. Okay so I guess we would do record username and password. Yeah.
> CP4-2: Ohhh okay. I gotcha.
> CP4-1: So, when you are setting your passwords you want the safety system to not interfere.... record...I think the same thing, the second one. Don't you? Don't you want to...

Citizenship entails rights and membership, similar to membership on a collaborative platform. When couples engage in collaborative negotiation of settings they are deciding terms for their mutual safety. Citizenship, as a metaphor for this system, entails empowerment through the creation of collaborative space.

5.2 Removing Barriers to Participation

For couples, removing barriers through participation in internet activities is understandably associated with greater autonomy and they are optimistic that they can manage settings based on their perceptions of how much oversite is needed to grant that autonomy. Couples preferred to grant as much independence as possible in the present and change settings only later, if or when circumstances appear to require it; and they felt that the spectrum of settings lent themselves well to this approach. Autonomy (that removes barriers) here is multifaceted referring to freedom from burden of oversite, ability to address issues in the absence of the other, and also feeling like they are independent online. This independence is integral to the open collaboration concept of providing less data, less commitment or identifying information (e.g., in the form of personal histories and approval of activities in situ) to the extent possible.

In general, the criteria for changing settings at some future time lacked specificity. Couples sometimes reflected on how their settings would need to change once memory concern progressed, yet they did not explicitly define the triggers or conditions that might require it. For this reason, participants sometimes suggested they would leave it to their couples to let them know when they felt unable to function adequately—even while sharing anecdotes about others for whom some kind of oversight might have prevented financial disaster. CP1 emphasized that for now, they were giving each other the autonomy they had always had, and would allow the other to signal when more oversight was needed:

> CP1-1: If we were feeling that one had more memory concern than what we are initially thinking, which she will get, and I will too ... she still can remember ... I think these are good questions [particularly] for someone in more dire straits than she is.

> Interviewer: Do you anticipate modifying these settings in the future?
> CP1-2: Probably.
> CP1-1: Yes, yes, definitely. We are in the first stages … I went with her trusting that she would remember.
> CP1-2: I forgot today.
> CP1-1: But she will forget … The ball is in her court until she starts to really forget […] Right now we are still in early stages. But I think those questions are good because they hit all bases. In later years, in later times, it may occur.

CP1 reiterates that they chose less stringent settings because they "trust" one of the couples "will remember." Like CP1, CP5 is not sure of when they can expect "it," (memory loss) but imagines they would adjust their Safety Settings if/when memory is "affected," without clarity as to how, illustrating the challenge for people to imagine themselves at a future point in time when capacities are diminished and the needed level of self-awareness for effective decision-making may be lost. Couples suggested that they would keep the settings less stringent but adjust as the partner declines. That is, they like that the system has a range of options because it prolongs independence:

> CP5-1: His memory may be affected more … So, we may adjust the settings.

CP2 reiterates that having Safety Settings are also important in cases where one of the two needs access, not just for reasons of memory loss, but simply to manage in the event that something happens to the other partner. That is, these settings remove barriers foreseen by the incapacity of another. In this particular instance detailed below, autonomy is shifted to the person with less concern about memory loss. CP2 points out that the sheer fact of their reliance on one another necessitates collaborative oversite, while acknowledging that their oversite is still hampered by their couples tendency to forget passwords:

> CP2-1: You know, you rely on one another and I think apps or things that could help you with managing things like passwords and certainly money we are handling fine but I can see a time where somebody might click on the wrong thing very innocently or maybe not so innocently and it could cause a big problem.
> CP2-1: My concern would be if [my partner] would pass today, I have a very loose idea of what his passwords would be and he changes them frequently because he has some difficulty remembering them.

Although CP2 likes the idea of oversite in case of an unexpected event, this concept of autonomy lowering barriers for both members of the couple is integral to the uncertainty of disease progression. While some couples are unwilling to estimate when progression might require some intervention, others speculate they may need to change Safety Settings in five to 10 years. Almost all acknowledge that the need for setting changes will depend on how fast one or both partners decline. Indeed, some say that if both were to decline, they would want family members to have access to their settings and the system. They nevertheless think of family access—like the need for more advanced Safety Settings—in a vague and indefinite way, leaving open the time frame or circumstances in which such access might be required. For example:

> CP3-2: So, it's just something that I think people need at a certain point. Because we really think about the possibility of future issues.

For now, couples are concerned with autonomy for both. While they want oversight, they also want to ensure that this oversight does not introduce unnecessary barriers.

One way that concern plays out is with respect to social media. When selecting Safety Settings for Facebook, for example, CP4 considers their different social habits and concludes that oversight would not work for them; it would create too many barriers:

> CP4-1: Yeah, how about the record all attachment button. The second one. Yeah. When you like a Facebook post… WHISPERING what should I say? We don't really do Facebook but let's see. When you like a Facebook post, you want the safety system to not interfere, record all Facebook likes, immediately notify…
> CP4-2: Immediately notify your partner that you liked a post and wait for his response to proceed.
> CP4-1: Hmmmm.
> CP4-2: Pick the third one. I mean unless you want…
> CP4-1: I don't want to do immediate stuff because we are always different.
> CP4-2: Okay, well then do that one.

Another example of this concern about partner burden (and thus, autonomy and barriers to participation) can be seen when CP2-2 worries that getting alerts may drive the other more advanced memory concern partner "crazy," suggesting a willingness to assume the responsibility for oversight more readily than they are ready to impose the burden on a partner. Indeed, couples rarely distinguish who the safety system is meant to support, sometimes acting as if they are making selections for themselves, rather than for the partner who is apparently more advanced.

Because couples acknowledge that memory concern is unpredictable and could affect either partner, they think of Safety Settings as meant for both. This willingness to embrace the fluidity of their roles created context for the decision process: the approach they took in selecting the Safety Settings; how they imagined they would use them in relationship to progression; and their assertion that the system would have to be on their terms in order for them to maintain full participation in their own lives.

Couples also did not want to encroach on the activities of their partner if there was no risk to them. This notion of collecting only what data you need is indeed a widely held opensource software value:

> CP3-1: Um, just not interfere. He doesn't care. We've been married [over 50 years].

Shortly after, CP3-2 (who has no memory concerns, and who has actually gone out of their way to communicate that) says jovially that they do not need permission to go online:

> CP3-2: I don't think I need your permission to go online, dear.

5.3 Maintaining Ongoing Contribution

The concept of nurturing ongoing participation relates to lowering barriers but moves beyond it in the sense that it sets up the terms of governance for sustaining partnership and maintaining or renegotiating sociotechnical roles. This reluctance to abandon roles meant that those with more memory concern nonetheless led the technical aspects of the setup and Safety Setting selection because that was their historic role in the partnership. Indeed, we drew the impression that couples either wanted to maintain their mutual agency or were maintaining the status quo in their sociotechnical relationships in order not to dislodge existing roles that extended beyond technical worlds.

Specifically, we found that individuals with potentially greater memory challenge or concern were more likely to lead the interview, including technical aspects like the remote setup and the safety setting selection. This may have reflected greater motivation or greater technological

sophistication, but regardless, is a reminder that relationship dynamics and established technology practices/roles will supersede other considerations.

For instance, the CP2 partner with more memory concerns (CP2-1) led the technology setup and walkthrough, projecting what may have been a habit of taking charge under such circumstances, even while consulting their partner at every turn:

> CP2-1: You don't want it to interfere, correct?
> CP2-2: . . . You should probably have some [safety checks here] because you always say to me did you click on a link when we end up some place, we are not supposed to. . .
> CP2-1: You want this?
> CP2-2: Yes, I'd like to record it and then if there's a problem you know what you've clicked on.

Sometimes conversations about Safety Settings between couples might start out more transactional and be peppered with statements that reiterated the need for independence and consideration for how the other thinks. CP1 was adamant about not interfering to maintain the level of autonomy that would, presumably, sustain full and independent participation:

While discussing Facebook settings:

> CP1-1: Like what you like.
> CP1-2 Do not interfere.

While discussing Banking settings:

> CP1-2: Separate accounts. Not interfere.

This is a topic that couples are exploring gently in their negotiations about Safety Settings, but with an understanding that how they organize themselves *now* will matter *later*. While members of the couple with less memory concern want to have confidence in whatever system they set up, they also want to make sure they are creating independence for their partner. They want a system that works for them as a couple.

In all of these interactions, relationship idiosyncrasies were readily exposed and playfully discussed—for instance, revelations about who knows how to set up the video conference, who is more organized, who is stubborn, who was right about anything in the first place, and so on. These historic personas seemed important for them to expose and reenact as they set about choosing settings, as if to ensure that their histories would not be lost or forgotten.

5.4 Couples in Cybersecurity: Diary Study

In our diary study, we learned that couples encounter external threats most often, but that they are perhaps most concerned with internal threats. External threats include emails from senders looking for couples to update account payments from accounts they do not have; emails from senders that are not the company represented (as discerned from the sender or link); and emails describing activities or requesting logins or password changes that couples knew (or, doubted) they had done. These external events garner feelings reported in their diaries of being "scared," "confused," "pissed," and "violated." External threats are typically detected and thwarted because couples are vigilant about notices referencing activities they did not initiate.

Internal threats, by contrast, describe events that couples acknowledge they regret, such as buying something from a "spammy" company; entering passwords incorrectly; falling for a shopping scam; posting something that they should not have on Facebook; or clicking on a link that they knew in retrospect was not legitimate or where they wanted to go. These events can result in

self-reproach ("I will not purchase from [seller] again") and conversation between couples dissecting what went wrong and how to mitigate it ("We agreed never to click on [suspicious links] again"). For example, CP3-1 mentions in her diary that her husband typed in the wrong URL for their banking site, which resulted in CP3-1 putting a shortcut to the banking site on her partner's browser. CP3-1 also initiated a warning for incorrect logins, increased security through two-factor authentication, and added other account alert features provided by their bank.

Couples collaborate differently around external vs. internal threats. For external threats, couples mostly describe in their diary merely mentioning it to their partner or doing nothing at all. CP5-1 often says in their diary, after, for example, a phishing encounter or a suspicious IM on Facebook, that they must "just be careful" or "keep vigilant." At most, both CP3-1 and CP5-1 do sometimes report in their diary that they "informed" their partner about an event they reported in the diary. CP2-1 reports occasionally venting "frustration" or sharing an incident to get input on what to do (e.g., "delete").

For internal threats, relationship dynamics and remedial steps are more front and center. Internal threats, more often result in teachable moments where couples engage in corrective actions (e.g., from the diary: "I re-showed him how to find his history of recent searches" or "I added the icon at the bottom of the computer for both of us to use in the future." (CP3-1). Couples might also just "explain to [their partner] what transpired" (CP2-1). On several occasions, CP5 reports in their diary that they are making a rule that they will not initiate activities without telling each other so that they have a shared set of facts. When CP5 discovers that one of them has received an email about gaming, they decide to delete the email and set a rule to not "click on any site related to gaming/gambling" (CP5). CP3-1 sternly reminds their partner that no email link is safe to click on (not even from their relative): "I reiterated to [partner] that he should NEVER click on a link in an email without checking with me or just not do it EVER. I explained the danger."

Over the course of this study, CP3-1 grows more concerned about her banking security because her husband enters passwords incorrectly or visits the wrong (suspect) banking URL—this was evident both in the diary and in our post interview. These incidents lead her to adjust their security at the bank and also internally (e.g., adding a shortcut to the bank URL to her partner's browser); they might also sometimes lead to more heated debate. Still, when we interviewed couples they were reluctant to change Safety Settings for the hypothetical system based on their experiences. Even though our study with these couples has taken place over the course of a year, it is possible that not enough cognitive change has passed for couples to feel that more restriction is necessary. It may also be that by providing couples with the structure to proactively think about and discuss threats (in this case, through the diary) that they felt comfortable managing their mutual security as they had been doing.

6 DISCUSSION

6.1 Service Provider-Contributor and Empowerment through Citizenship

The range of choices we provided have the potential to preserve autonomy and internet participation for both couples. Record-keeping measures like a *log* extend versatility and adaptability of purpose, in the sense that couples may initially conceive of them as a way to preserve self-oversight and, only later, as a way to maintain *partner*-oversight. On collaborative platforms like Wikipedia, the community has access to known contributor logs in order to maintain discrete histories of contribution and thus, give contributors access as to full citizenship—and the agency and recognition that documented contribution entails. Those platforms also provide contributors with access to their own participation, which is critical for growing and sustaining full membership [10]. In their own smaller collaborative space, our couples seem to find features like logs, which provide

social translucence [37] to be empowering. In addition, public collaborative platforms provide administrators with certain types of access, which can be activated when situations escalate. Again, for our couples, features giving other designated individuals access to records of activities (either theirs or their partner's) were seen as critical for comanagement of cybersecurity, even without the threat of memory concerns, and they certainly seemed important backstops for a time when memory might fail both couples, requiring more extensive support or oversight.

Collaborative, opensource environments are designed in such a way as to *lower barriers* for users whom they hope will become members (or citizens) by requiring them to give up only as much information as they are comfortable doing, thus encouraging them to participate on *their terms*. Because collaborative service provider models are dependent on volunteer contributors, they are more willing to adapt to the contribution behaviors and conditions of their users. The emphasis in open collaboration environments on *sustaining participation* by encouraging independence—and thus, citizenship—is an important lens as well. Each of these findings we have framed support a kind of citizenship in which one has the right to contribute, their dignity is preserved and participation is flexible, where sustained cooperation is necessary for conferring those rights, and where some amount of social translucence (or surveillance) is required for the safety of all.

In our diary study, we learned that couples may know how to increase security on their bank accounts or make connections between purchase behavior and a barrage of spam, but they are also juggling the uncertainty of what they or their partner might do—even if it is not necessarily clear how much is related to cognitive change. Sometimes they feel ashamed and remorseful, other times frustrated or mad, both of which are helped by venting to the partner. The constant among these incidents is the need for awareness and to discuss and learn from each other as these events occur. A system that promotes reflection and mutual oversight could provide that kind of transparency and the permission structure to talk more regularly about security threats from within and without that are so necessary for citizenship we describe. It will be important to create opportunities for couples to engage in reflection on what has transpired. While couples seem innately skeptical of communications about services they did not initiate or things they did not do (e.g., logging in to a service, signing up for an account) external threats can sometimes require support from family members like children. It may be useful to provide those designated individuals with oversight that might help them provide guidance and support. Thinking about this as a collaborative enterprise thus helps to extend responsibility to family members who may even be able to further extend independence.

In our early prior work, we spoke with those with MCI and explored the importance of equity in the face of identity loss [34] and also learned that in making decisions about cybersecurity couples want to address safety concerns and memory challenges in a collaborative way but lacked the options to do so [40]. Over time, as we spoke with couples and conducted several studies, we learned about their rich sociotechnical and collaborative dynamic. The importance of investing in cooperation that Piper et al. emphasize [45] was reenforced. Yet, collaboration does not ensure certain rights and equal membership. Thinking about this as a collaborative community and with both members of a partnership as *equal* members, gives responsibility back to the individual whose autonomy may have been compromised by creating a space (like opensource collaborative environments) that are built to accommodate changes in contribution, ability, and sustained engagement. If we consider that suffering from memory loss may be somewhat like a contributor whose skills and attention are unpredictable, we invite systems that not only ensure equal membership or citizenship, we also support the collaboration that couples so desire but struggle with because their options for security lack nuance and flexibility [41].

In our diary study with couples, we learn how much time they dedicate to discussing events that have happened online and creating rules for dealing with them. Creating a repository where

they can see what each other are doing and also give them the control to flexible adjust safeguards seems well suited to ameliorate this dynamic. We introduced a technology probe and a diary study to explore the collaborative nature of decision-making and specifically how much choice and flexibility couples want; and we ultimately explored scenarios that supported the design of a Safety Settings application [39]. The theme that we returned to, and which is formalized in this article, is the desire for collaboration and identity and autonomy preserving system that is imbued with a sense of how power, agency, and societal structures can thwart even the best intentions. Our framework of citizenship and open collaboration (which we discuss in more depth in the next section) is a useful model for design in that it emphasizes investment in collaborative community building and for roles, at any given time, to change. Our Safety System design is invested in cooperative enterprise that extends citizenship to individuals whose autonomy may seem to fall outside of normative frames and suffer as a consequence.

6.2 Further Reflection on Citizenship and Open Collaboration

In modern liberal democracies, the concept of citizenship presumes some claim on support from the state in the form of a social safety net, along with more fundamental privileges of democratic participation, equality of opportunity, and equal protection under the law. But even in democratic societies, modern notions of citizenship are complex and controversial, since citizenship is not just a public idea but a personal one, putting principles in conflict with lived experience. Citizenship has been explored in numerous studies in HCI and related social computing disciplines, many of them focusing on how to use technology to foster participatory commitments associated with legal citizenship. For collaborative or collective perspectives on citizenship, we might turn to Walzer, whose theory about the "unique set of norms of justice" [43] rests on the dominant view of justice held by a community. Theories about internet privacy, in particular, have built on Walzer's thinking, with arguments that privacy is contextual and is ultimately decided by communities of individuals with a shared membership and shared set of norms and privacy expectations. In our view, the notion of citizenship is most powerful when it can be extended to include dynamic configurations—couples or family units that fall outside the norm (in this case, because one or both do not fulfill societal standards of "normal" cognition). We think of our technology intervention as cooperative infrastructure and a site of power, agency, and politics, which can be oppressive, but which can also make social change possible. Indeed, since the technology may introduce tradeoffs in the form of heightened surveillance, we have learned that a continuing sense of agency and the potential to reverse oversight remains important (e.g., both couples want the ability to turn logs off [39]). Of course, citizenship is intricately interwoven with surveillance (discussed more in the next section), particularly in times of health and national security crisis [29], or in situations when a member of the family is experiencing cognitive change. Our future designs will continue to grapple with the freedoms that citizenship-surveillance affords.

By applying the lens of citizenship, we build on Bartlett and O'Connor [2], who emphasize the importance of social structures that have placed limits on individual agency. We consider not only power and agency but also the changes, resulting from surveillance capitalism, in perceptions of privacy and security risk that may lead people to be, on the one hand, more permissive of surveillance and, on the other, more concerned about cybersecurity breaches. Yet there is reason to be wary of theories that are based on membership as they can reenforce exclusion and control. When combined with the concept of open collaboration, citizenship transforms the thinking about the individual as one who not only is entitled to the same rights as other citizens but can actually realize them through collaborative infrastructures. For our purposes, thinking about citizenship in the context of open collaboration (although an imperfect metaphor) allows us to consider what rights individuals are entitled to and what structures might support those rights, in particular

knowing that with aging populations and cognitive challenges, there is a tendency to "fix" the problem using normalized structures that compromise citizenship. As Mentis et al. find, sometimes restricting rights is the only thing one (feels they) can do [41]. Without support, this may be inevitable. But if we think of security as shared project that requires collaborative and adaptative solutions from members of a partnership working to preserve each other's rights, attempts to enhance security are most appealing when they honor and perpetuate existing rights and roles rather than altering them.

Because open collaboration environments promote self-direction and limited involvement, it would appear that this frame of citizenship and collaboration is a useful way to think about the domestic partnerships we studied; easy membership. Each of the relevant goals (histories, lower barriers, and sustaining contribution through autonomy) has applications for the cybersecurity dynamic of these couples. This model helps to reframe the relationship from "patient" to partnership in a collaborative enterprise. The couples we studied demonstrate that is not necessary for one to monitor the other at stages in which varying degrees of participation remain feasible for both. It is important to avoid imposing a false power structure featuring consistent subordination of one by the other in cybersecurity oversight. A participatory citizenship model is not only more closely aligned with social reality; it may help sustain that participatory reality for a longer period of time by encouraging collaboration rather than suppressing it. By thinking about this through the frame of citizenship we consider not only a model for thinking about those with cognitive challenges as deserving of help, but of rights to use the internet—as a whole human being whose autonomy can be sustained (perhaps not indefinitely but longer). If we exchange normative frames (as Bartlett and O'Connor suggest) for how individuals must typically use the internet for a collaborative configuration, we might provide the basis for citizenship. A system that is designed using collaborative architectures and that elicits mutual reflection and discovery of challenges and provides measured steps is one that better fulfills this model. Ultimately, when it comes time to negotiate a shared life that involves mutual assets the model of citizenship and open collaboration fits well when we consider other practical configurations around partnership. Partnerships may be defined by emotional bounds, but financial and administrative concerns are usually very present—and they require additional administrative care.

Our research is focused on how to extend membership for those who have been experiencing cognitive change, while acknowledging that changes in cognition may require more robust collaborative frames. There is a paradox: in trying to escape the problem, couples are given tools that produce new forms or variations on the problem. There is hard work that goes into being aware and accountable for the other, but also too in making those activities visible and collaborating for the sake of accountability or health of the couple. We do not necessarily resolve these issues with this set of studies, but we do provide more insight into the needs of a collaborative community, in this case, members of a couple experiencing cognitive changes.

6.3 Vulnerable Cybersecurity

In experimenting with a technology that provides couples with surveillance mechanisms for addressing memory and cognitive decline, we observed that the concept of surveillance technology raised few alarms with participants. This is consistent with a troubling trend in many sectors toward the normalization of surveillance, in exchange for the ostensible benefit of being better able to manage various aspects of life. Ironically, people may perceive or experience the loss of control implied by surveillance as a form of increased control. We are reminded that exertion of agency takes many different, sometimes competing, forms involving tradeoffs based on complex personal risk assessments. While believing that this type of technology can help older couples cope with memory concern, we are also cognizant of its potential risks and abuses. Indeed, Piper et al. has

drawn attention to the importance of cooperative experiences are balanced with ethics [45]. For Piper et al., designs that are cooperative support dynamics among dyads [45] which previous work focused on couples in offline settings have emphasized [25, 26].

The ability to backstop failing memory with a record of steps results in trace data that would leave couples potentially vulnerable to surveillance and theft. When reframed as a kind of collaborative service provider model, this technology may be designed in ways that keep couples safer from adversaries of any kind by enlisting them in mutual oversight and community partnership. We may be able to draw added value from this conception if it inspires us to borrow relevant cybersecurity protocols for effective use in domestic partnerships—especially those with limited resources to manage an elevated level of risk. Older adults are key examples.

6.4 Future Work and Implications

We have since engaged couples in future protypes that ground couples in the experience of decision-making around these settings. We learned what kinds of information they want in their logs that will help them mutually manage oversight and how it varies depending on memory loss and/or sociotechnical dynamics. We designed these logs to support a collaborative opensource model whereby couples could be aware of what the other is doing and take action to adjust settings accordingly. We also do not restrict roles so that no one person is running the system, rather the couple has access to their mutual histories and settings.

Our next step will be to trial the system with couples. Some questions we will ask: Do couples in fact monitor each other, and do their roles in oversight change (and in unpredictable ways)? Do they collaboratively make decisions together about Safety Settings and changes to those settings *in situ*, and when given the option to flexibly customize Safety Settings, are those decisions more modest (e.g., restrict a link vs. all links) than when they had fewer options? Do couples tolerate oversight such as immediately alert or review activities in their day-to-day lives? How will they negotiate, for instance, lags in response? Moreover, in light of some of our concerns about surveillance, will couples ultimately find these settings too intrusive? We will be exploring these and other questions raised by this research in future iterations of this design.

7 CONCLUSIONS

Our findings lend support to the idea that aging couples in need of enhanced support to manage their online interactions are both drawn to, and potentially best served by, approaches to cybersecurity that treat them as a collaborative community of participants with the latitude to set personally acceptable and mutually agreed-upon terms of participation. Use of this model as a frame for consideration of cybersecurity tools will advance both the level of protection conferred and the level of citizenship each partner is capable of exercising. This research reminds us that these partner collaborations are not always governed by a memory status hierarchy; they also reflect a history of negotiated roles and interactions, which the couples will tend to honor in their methods of deliberation and in the decisions they make. Consistent with that finding, our work also highlights partner's sensitivity to the need to balance autonomy with oversight in a way that respects the integrity of the relationship. And finally, it underscores their appreciation for protections that offer the flexibility to accommodate not just divergent personal styles and needs, but also changing circumstances, given the inherently dynamic nature of cognitive decline and the implications for both online efficacy and cybersecurity needs.

There are, of course, limits to citizenship as a metaphor in that it deals with membership, and that is a privilege that is traditionally not conferred on all equally, which is why we draw on metaphor of collaborative design. Individuals with memory changes are subject to structural discrimination

and essentialist logic about personhood that making any step toward theorizing about citizenship and restoring rights to be critical.

APPENDIX

[Google Form Diary Questionnaire]

Cyber-Safety Event Diary

Thanks for being part of our diary study! We will be asking you to provide entries on a regular basis for the next month. Our goal is to learn about the privacy or security challenges you encounter as you go about your daily routine and have you reflected on them with our guided prompts as close to the event as possible.

Every time you have encountered an event like the ones we describe (below) or something else that makes you feel insecure or worried about your cybersecurity, we would like you to make an entry into the journal by filling out this Google form and submitting it. Once we see that you have submitted, we may follow-up to learn more.

_____

Email

_____

_____

Please enter the date.

_____

_____

Please give the event a short description.

_____

_____

_____

We are going to ask you to describe the event in greater detail, but we would first like to know, does the event fit any of these descriptions? Please indicate which one(s).

- ☐ Received/clicked on an email link that I/my partner suspect or know was phishing
- ☐ Received/clicked on an email attachment that I/my partner suspect or know was phishing
- ☐ Liked a link on Facebook that I /my partner suspect or know was malicious or embarrassing
- ☐ Posted something on Facebook that I/my partner should not have or regretted
- ☐ Went to banking site that I/my partner suspect or know was not the real site (e.g., spoofed site)
- ☐ Entered sensitive data into a banking site that I/my partner suspect or know was not the real site (e.g., spoofed site)
- ☐ Transferred money to someone I/my partner should not have
- ☐ Went to shopping site that I/my partner suspect or know was not the real site (e.g., spoofed site)
- ☐ Entered sensitive data into a shopping site that I/my partner suspect or know was not the real site (e.g., spoofed site)
- ☐ Made a purchase on a shopping site that I/my partner should not have or regretted
- ☐ Received notification of a password breach I/my partner suspect or know was the result of someone else changing my/our password
- ☐ Could not get into a site with my/our password and had to change it

☐ Was browsing and I/my partner got lost and did not know how to find the site again
☐ Downloaded a file that I/my partner should not have
☐ Other: _____

_____

Could you describe what happened in as much detail as you can? For instance, what made you suspicious or worried?

_____
_____
_____

At the time when this event occurred, please tell us in your own words how this made you feel?

_____
_____
_____

Please indicate how this event made you feel about your online safety?

- ○ Not at all concerned
- ○ Slightly concerned
- ○ Somewhat concerned
- ○ Very concerned

_____

During/after this event what, if any, steps did you take to learn more or alleviate/confirm your concerns? For instance, did you contact the business or sender? Did you report the email or website? Did you research the link, sender, or business? Please describe ANY steps you took.

_____
_____
_____

What, if anything, did you say to your partner about what happened with regard to this incident?

_____
_____
_____

Do you think this event will lead you to change anything you do online? If so, please tell us how?

_____
_____
_____

You can upload examples of events here (e.g., screen shots or PDFs of emails)

[Add file]

REFERENCES

[1] I. Altman. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. Brooks/Cole.
[2] R. Bartlett and D. O'Connor. 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/10.1007/s10676-012-9286-x
[3] R. Batchelor, A. Bobrowicz, R. Mackenzie, and A. 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 (Jun. 2012), 99–108. DOI: https://doi.org/10.1007/s10676-012-9286-x

[4] E. P. S. Baumer and J. R. Brubaker. 2017. Post-userism. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 6291–6303.

[5] T. Bielsten and I. Hellström. 2017. A review of couple-centred interventions in dementia: Exploring the what and why—Part A: Dementia. 18, 7 (Nov. 2017), 2436–2449. DOI: https://doi.org/10.1177/1471301217737652

[6] K. Boehner, J. Vertesi, P. Sengers, and P. Dourish. 2007. How HCI interprets the probes. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 1077–1086.

[7] V. Braun and V. Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (2006), 77–101. DOI: https://doi.org/10.1191/1478088706qp063oa

[8] A. Brooke and L. Raine. 2019. *Key Takeaways on Americans' Views About Privacy, Surveillance and Data-Sharing*. Pew Research Center.

[9] A. Bruckman. 1993. Gender swapping on the internet. In *Proceedings of INET'93*.

[10] S. L. Bryant, A. Forte, and A. Bruckman. 2005. Becoming Wikipedian: Transformation of participation in a collaborative online encyclopedia. In *Proceedings of the 2005 ACM International Conference on Supporting Groupwork*. 1–10.

[11] M. Burawoy. 1998. The extended case method. *Sociological Theory* 16, 1 (1998), 4–33.

[12] D. K. Citron and B. Wittes. 2017. The internet will not break: Denying bad Samaritans section 230 immunity. *Fordham Law Review* 86, 2 (2017), Article 3.

[13] J. Clifford and G. E. Marcus. 1986. *Writing Culture: The Poetics and Politics of Ethnography: A School of American Research Advanced Seminar*. University of California Press.

[14] P. Dourish. 2014. Reading and interpreting ethnography. In *Ways of Knowing in HCI*. Springer-Verlag, 1–23.

[15] P. Dourish. 2007. Responsibilities and Implications: Further thoughts on ethnography and design. In *Proceedings of the 2007 Conference on Designing for User eXperiences*. 25:2–25:16.

[16] T. Erickson and W. A. Kellogg. 2000. Social translucence: An approach to designing systems that support social processes. *ACM Transactions of Computing-Human Interaction* 7, 1 (Mar. 2000), 59–83. DOI: https://doi.org/10.1145/344949.345004

[17] Facts and Figures. Retrieved 2019, from https://alz.org/alzheimers-dementia/facts-figures.

[18] S. Fazio, D. Pace, J. Flinner, and B. Kallmyer. 2018. The fundamentals of person-centered care for individuals with dementia. *The Gerontologist* 58, suppl_1 (Jan. 2018), S10–S19. DOI: https://doi.org/10.1093/geront/gnx122

[19] A. Forte and C. Lampe. 2013. Defining, understanding and supporting open collaboration: Lessons from the literature. *American Behavioral Scientist* 57, 5 (2013), 535–547. DOI: https://doi.org/10.1177/0002764212469362

[20] D. Freed, J. Palmer, D. Minchala, K. Levy, T. Ristenpart, and N. Dell. 2018. "A stalker's paradise": How intimate partner abusers exploit technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–13.

[21] R. S. Geiger and D. Ribes. 2010. The work of sustaining order in Wikipedia: The banning of a vandal. In *Proceedings of the 2010 ACM Conference on Computer Supported Cooperative Work*. 117–126.

[22] G. R. Hayes. 2014. *Knowing by doing: Action research as an approach to HCI. In Ways of Knowing in HCI*. J. S. Olson and W. A. Kellogg (Eds.), Springer, 49–68.

[23] G. R. Hayes. 2011. The relationship of action research to human-computer interaction. *ACM Transactions on Computer-Human Interaction* 18, 3 (Aug. 2011), 15:1–15:20. DOI: https://doi.org/10.1145/1993060.1993065

[24] D. Heater. 2013. *What is citizenship?* John Wiley & Sons.

[25] I. Hellstrom, M. Nolan, and U. Lundh. 2007. Sustaining "couplehood": Spouses' strategies for living positively with dementia. *Dementia* 6, 3 (2007), 383–409.

[26] I. Hellström, M. Nolan, and U. Lundh. 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

[27] D. Hornung, C. Müller, I. Shklovski, T. Jakobi, and V. Wulf. 2017. Navigating relationships and boundaries: Concerns around ICT-uptake for elderly people. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 7057–7069.

[28] A. S. Hwang, P. Jackson, A. Sixsmith, L. Nygård, A. Astell, K. N. Truong, and A. Mihailidis. 2020. Exploring how persons with dementia and care couples collaboratively appropriate information and communication technologies. *ACM Transactions on Computer-Human Interaction* 27, 6 (Nov. 2020), 46:1–46:38. DOI: https://doi.org/10.1145/3389377

[29] S. E. Igo. 2018. *The Known Citizen: A History of Privacy in Modern America*. Harvard University Press.

[30] M. S. Jørgensen, F. K. Nissen, J. Paay, J. Kjeldskov, and M. B. Skov. 2016. Monitoring children's physical activity and sleep: A study of surveillance and information disclosure. In *Proceedings of the 28th Australian Conference on Computer-Human Interaction*. 50–58.

[31] A. Lazar. 2014. Using technology to increase meaningful engagement in a memory care unit. In *Proceedings of the 18th International Conference on Supporting Group Work*. 255–257.

[32] A. Lazar, C. Edasis, and A. M. Piper. 2017. A critical lens on dementia and design in HCI. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 2175–2188.

[33] A. Lazar, C. Edasis, and A. M. Piper. 2017. Supporting people with dementia in digital social sharing. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 2149–2162.

[34] G. Madjaroff and H. Mentis. 2017. Narratives of older adults with mild cognitive impairment and their caregivers. In *Proceedings of the 19th International ACM SIGACCESS Conference on Computers and Accessibility*. 140–149.

[35] D. Mahoney, R. Purtilo, F. Webbe, M. Alwan, A. Bharucha, T. Adlam, H. Jimison, B. Turner, and S. Becker. 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, 3 (Aug. 2007), 217–226. DOI: https://doi.org/10.1016/j.jalz.2007.04.388

[36] A. Marwick and boyd danah. 2010. I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society* 13, 1 (2010), 114-133. DOI: https://doi.org/10.1177/1461444810365313

[37] D. W. McDonald, S. Gokhman, and M. Zachry. 2012. Building for social translucence: A domain analysis and prototype system. In *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work*. 637–646.

[38] N. McDonald, A. Larsen, A. Battisti, G. Madjaroff, A. Massey, and H. Mentis. 2020. Realizing choice: Online safeguards for couples adapting to cognitive challenges. In *Proceedings of the 16th Symposium on Usable Privacy and Security (SOUPS'20)*. 99–110.

[39] N. McDonald and H. M. Mentis. 2021. Building for "We": Safety settings for couples with memory concerns. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems*.

[40] H. M. Mentis, G. Madjaroff, A. Massey, and Z. Trendafilova. 2020. The illusion of choice in discussing cybersecurity safeguards between older adults with mild cognitive impairment and their caregivers. In *Proceedings of the ACM Conference on Computer-Supported Cooperative Work & Social Computing*.

[41] H. M. Mentis, G. Madjaroff, and A. K. Massey. 2019. Upside and downside risk in online security for older adults with mild cognitive impairment. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 343:1–343:13.

[42] Mild Cognitive Impairment—Symptoms and Causes. *Retrieved* 2019, from https://www.mayoclinic.org/diseases-conditions/mild-cognitive-impairment/symptoms-causes/syc-20354578.

[43] H. Nissenbaum. 2004. Privacy as contextual integrity. *Washington Law Review* 79, 1 (2004), 101–139.

[44] L. Palen and P. Dourish. 2003. Unpacking "privacy" for a networked world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 129–136.

[45] A. M. Piper, R. Cornejo, L. Hurwitz, and C. 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)*. 5311–5323.

[46] Y. Rogers. 1997. Reconfiguring the social scientist: Shifting from telling designers what to do to getting more involved. In *Social Science, Technical Systems, and Cooperative Work: Beyond the Great Divide*. Psychology Press.

[47] J. Ruby (Ed.). 1981. *A Crack in the Mirror: Reflexive Perspectives in Anthropology*. University of Pennsylvania Press.

[48] P. S. Sachdev et al. 2015. The Prevalence of Mild Cognitive Impairment in Diverse Geographical and Ethnocultural Regions: The COSMIC Collaboration. *PLoS ONE* 10, 11 (Nov. 2015). DOI: https://doi.org/10.1371/journal.pone.0142388

[49] A. Schutz. 1967. *The Phenomenology of the Social World*. Northwestern University Press.

[50] S. L. Star. 1999. The ethnography of infrastructure. *American Behavioral Scientist* 43, 3 (Nov. 1999), 377–391. DOI: https://doi.org/10.1177/00027649921955326

[51] L. A. Suchman. 1987. *Plans and Situated Actions: The Problem of Human-Computer Communication*. Cambridge University Press.

[52] B. Tejada-Vera. 2013. Mortality from Alzheimer's disease in the United States: Data for 2000 and 2010. *NCHS Data Brief* 116 (Mar. 2013), 1–8.

[53] Christopher Parsons, Adam Molnar, Jakub Dalek, Jeffrey Knockel, Miles Kenyon, Bennett Haselton, Cynthia Khoo, and Ron Deibert. 2019. *The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry*. Retrieved 2019, from https://citizenlab.ca/2019/06/the-predator-in-your-pocket-a-multidisciplinary-assessment-of-the-stalkerware-application-industry/.

[54] S. Turkle. 1997. *Life on the Screen: Identity in the Age of the Internet*. Simon & Schuster.

[55] D. Unbehaun, K. Aal, R. Wieching, V. Wulf, D. D. Vaziri, S. Jahnke, and B. Wulf. 2019. Development of an ICT-based training system for people with dementia. In *Proceedings of Companion Publication of the 2019 on Designing Interactive Systems Conference 2019 Companion*. 65–68.

[56] J. Vines, G. Pritchard, P. Wright, P. Olivier, and K. Brittain. 2015. An age-old problem: Examining the discourses of ageing in HCI and strategies for future research. *ACM Transactions on Computer-Human Interaction* 22, 1 (Feb. 2015), 2:1–2:27. DOI: https://doi.org/10.1145/2696867

[57] A. F. Westin. 1967. *Privacy and Freedom*. Atheneum.

[58] What Is Mild Cognitive Impairment? Retrieved 2019, from https://www.nia.nih.gov/health/what-mild-cognitive-impairment.

[59] P. Wisniewski, A. K. Ghosh, H. Xu, M. B. Rosson, and J. M. Carroll. 2017. Parental control vs. teen self-regulation: Is there a middle ground for mobile online safety? In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*. 51–69.

[60] J. Zimmerman and J. Forlizzi. 2014. Research through design in HCI. In *Ways of Knowing in HCI*. J. S. Olson and W. A. Kellogg (Eds.), Springer, 167–189.

[61] S. Zuboff. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.

Received December 2020; revised May 2021; accepted May 2021