Realizing Choice: Online Safeguards for Couples Adapting to Cognitive Challenges

Nora McDonald, Alison Larsen, and Allison Battisti, *University of Maryland, Baltimore County;* Galina Madjaroff, *University of Maryland;* Aaron Massey and Helena Mentis, *University of Maryland, Baltimore County*

https://www.usenix.org/conference/soups2020/presentation/mcdonald

This paper is included in the Proceedings of the Sixteenth Symposium on Usable Privacy and Security.

August 10–11, 2020

978-1-939133-16-8

Open access to the Proceedings of the Sixteenth Symposium on Usable Privacy and Security is sponsored by USENIX.

Realizing Choice: Online Safeguards for Couples Adapting to Cognitive Challenges

Nora McDonald, *University of Maryland, Baltimore County (UMBC)* Alison Larsen, *UMBC*
Allison Battisti, *UMBC* Galina Madjaroff, *University of Maryland*. Aaron Massey, *UMBC*
Helena Mentis, *UMBC*

Abstract

This paper investigates qualitatively what happens when couples facing a spectrum of options must arrive at consensual choices together. We conducted an observational study of couples experiencing memory concerns (one or both) while the partners engaged in the process of reviewing and selecting "Safety Setting" options for online activities. Couples' choices tended to be influenced by a *desire to secure shared assets* through mutual surveillance and a *desire to preserve autonomy* by granting freedom in social and personal activities. The availability of choice suits the uneven and unpredictable process of memory loss and couples' acknowledged *uncertainty about its trajectory,* leading them to anticipate changing Safety Settings as one or both of them experience further cognitive decline. Reflecting these three decision drivers, we conclude with implications for a design system that offers flexibility and adaptability in variety of settings, accommodates the uncertainty of memory loss, preserves autonomy, and supports collaborative management of shared assets.

1. Introduction

While having choice may enable people to identify more avenues for securing their privacy and safety online, scholars worry that this could create a false sense of agency [2]. With the flood of Internet of Things (IoT) and mobile devices, our digital records are increasingly being mined in ways that expose us to unprecedented theft [31]. "Notice and choice" models are not only insufficient to our information age [11]; they may also promote a fallacy of individual control [20] while subverting the role of collaborative oversight [5].

This issue is even more pronounced for an aging population subject to cognitive challenges. As dementia slowly becomes a global epidemic, it is estimated that the condition will affect roughly 115 million by the year 2050 [13]. Alzheimer's dementia is a common cause of age-associated memory loss, though not the only one [30, 37, 44]. Although the prevalence of Alzheimer's in the United States may vary quite a bit [37], recent estimates suggest that over five million people in the United States suffer from the disease [14, 41].

In addition to producing serious deficits in quality of life for those who experience it, memory loss takes an enormous emotional and economic toll on over 16 million unpaid caregivers in the United States every year [9]. Those are people to whom much of the responsibility for the support of safe online activities on social networks, email, and banking and shopping sites falls [6, 25, 36]. Yet, informal caregivers may feel they cannot adequately regulate online practices, which in turn may lead them to restrict online activities for cognitively-challenged partners (or cognitively challenged family members) in a way that may do further harm to the individual [29, 36].

Tools are emerging that help people seemingly exert more control over their networked privacy and security settings, exist more ephemerally on their social networks [45], and delete browsing and other location data [4]. But managing one's own privacy-related stress and sense of helplessness is difficult [8], to say nothing of the stress and helplessness those struggling with memory impairment (and those struggling to safeguard them) may experience. Having an intermediary assist in negotiating this space, such as one's spousal partner, may be useful, but it also creates new and complex interpersonal and cooperative challenges. It may also require more data generation and storage and less privacy in order to allow partners to retrace the digital steps of those with memory impairment. Better understanding of how safeguards are negotiated with respect to privacy between partners will allow us to design better technology solutions.

Because we wanted to capture how Negotiation Partners (NPs) manage the sociotechnical challenges of choosing online safety settings in the face of cognitive challenges, we sought out individuals who had concerns about their memory, or the memory status of their loved one, and also had associated concerns about their safety online. We presented NPs with a "Safety Settings" web page that offered a choice of safety-enhancing browser extensions to help the partners manage online activities. Our findings are that NPs generally chose the security options that were less overbearing and created more agency for both of them, but in making these decisions, took account of context in a customized way, depending on a number of factors. First, NPs' choice of Safety Settings is influenced by both their desire to secure

USENIX Symposium on Usable Privacy and Security (SOUPS) 2020. August 9 -- 11, 2020, Virtual Conference.

shared assets and their individual and collective technology habits and preference (e.g., one has a system for passwords, the other doesn't). Second, their perceived concerns are rooted in a desire to preserve autonomy wherever possible. The importance of choice is heightened by a desire to develop a strategy that serves memory-challenged partners on their own terms, accommodating the degree of memory loss as well as their lifestyle and baseline technology aptitudes and needs. Third, NPs acknowledge the unpredictability of memory loss and the fluidity of their shifting memory-related roles. This sensitivity to the uncertain course shapes their approach to selecting safety settings: they tend to think of these settings as conferring benefits on both partners. Further memory loss motivates their desire for an adaptive system that poses a variety of choices.

Our paper makes the following contributions. First, we establish that key factors driving choice (securing shared assets, autonomy, and fluidity or instability of roles) are favorable to collaborative approaches to cybersafety. Second, we demonstrate how uncertainty in the context of memory loss is well aligned with choice. Third, our work highlights the need for designs that balance autonomy with collaborative protection of shared assets and risk. In the related work section that follows, we consider individual choice and service provider models as well as studies of memory concern and technology to situate our study. We then describe our study design and findings, and we conclude with recommendations for future work and design.

2. Related Work

2.1. Framing of user choice and service provider paradoxes

Our current internet service provider model is built on the idea that, as long as users are given a choice about whether or not they want to provide data, they are sufficiently protected. Even while scholars have long since acknowledged that "notice and choice" is woefully insufficient [10, 42], there is also recognition that, from a regulatory perspective, the model is here to stay [19]. Technology designers have begun incorporating "notice and choice" style privacy into the engineering process [38, 40], often with the encouragement of regulators [12]. For the foreseeable future, users of information systems must be able to make meaningful choices to manage their privacy.

Many companies, however, are choosing to bury privacy-focused options in so-called dark patterns that users are unlikely to be aware of, or able to defend against [18]. Others simply count on framing privacy choices to encourage well-known paradoxical user behavior in making privacy choices [1]. The privacy community may be unanimous in believing that users cannot, nor should not, be required to read privacy policies. The result is that "choice" has become a dubious concept [46]. The "choice" envisioned 50 years ago by regulators is now rather illusory.

This environment does not bode well for older, cognitively impaired individuals who may be dependent on their partners for privacy and security. Some scholars have observed that couples are making privacy and security decisions jointly, rather than, as most systems assume, individually. Recognition of actual information practices must result in reevaluation of the designs and assumptions that led to them. For example, password sharing practices have been studied in some detail [23, 39], leading to meaningful changes in policy [17].

Shared oversight may be a solution to joint management, but it too has problems. Acquisti et al. [2] identify three themes in surveying the privacy literature to address this question, notably taking up the issue of choice as a third constellation in which users have merely the *illusion of choice* due to subtle machinations that enhance or stifle privacy concerns. Those overarching vulnerabilities raise interesting questions. When a partner is making privacy decisions on behalf of a dyad, are they any better-equipped to see realistic options? Is it realistic to think of them as a bulwark that further fortifies the other user (or both of them) against manipulations?

There is an inherent paradox introduced by security. Measures taken to enhance it sometimes, though not always, have the effect of limiting privacy. Typically, a service provider who affords the platform, tools, and policies, organizes and monitors our data to prevent its misuse. They provide, for example, protection against scams or data theft. But the notion of couples exercising surveillance over one another is unique, even if there are corollaries, because these attempts to exercise protection fall outside normative models of privacy. Analogs like the monitoring of children and survivors of intimate partner surveillance/violence (IPS/V) usefully apply and are discussed in the next section. The caregiver who is theoretically tasked with taking on some of the burden of oversight of privacy and security must also oversee the couple's mutual security, which is to say, they are functioning in some ways like the service provider.

2.2. Finding a balance: safety versus surveillance

Theories like boundary regulation [3], the privacy paradox [24], and contextual integrity [32] have usefully described how individuals and communities manage privacy. Yet, what of couples trying to manage their privacy and security collaboratively? While privacy is an important value (though arguably not fully addressed by these theories), it is complicated by the desire to provide autonomy to individuals who are losing their memory. Boundary regulation [3, 35] assumes that the individual has the power and privilege to regulate access to the self, which individuals suffering from memory loss may not. Moreover, it assumes that regulating access to the self is the path to autonomy, when in fact, giving up some unedited activity (or sharing it with a partner or caregiver) may be what is required to gain autonomy.

Sometimes guardrails that introduce some type of oversight or surveillance may be the only approach that is both safe and empowering.

These checks and balances exist for other unique vulnerable groups, like children experiencing parental monitoring, who may find it restrictive and harmful [16]. There are also concerns, in this realm, that networked surveillance tools, some of which are used in parental monitoring [33], are also being adopted by those who perpetrate IPV and IPS [15, 43]. Parental monitoring and IPV/S are not the same as safety for elderly NPs with memory concerns, but arguably developers should be responsible for the intended uses *and actual uses* of technologies [33]. Our research attempts to understand the extent to which NPs are bound by these systems, how decisions are being made and by whom, what terms are acceptable, and whether or not NPs have concerns about surveillance. Unlike parental monitoring or IPS/IPV, the need to regulate a partner's activities is theoretically premised on a need to safeguard shared data and data linkage while maintaining autonomy. But like child monitoring, and maybe IPS/IPV, these monitoring activities nevertheless invite non-normative models for thinking through the problem, precisely because of dual use risks and vulnerability.

Couples where one or both has undiagnosed memory loss or MCI exemplify a unique cybersecurity and privacy problem. They may be even a discursive element in some areas of privacy studies because, for the sake of their cybersecurity, certain aspects of their privacy may be compromised in the service of their individual autonomy and mutual security. As with children and IPV and IPS survivors, what makes these mechanisms for security and cybersecurity valuable (e.g., find me or my phone) or convenient (e.g., storage backup) may, in fact, be what makes them prone to abuse by family/parents or intimate partners. It is this paradox that we enter, as researchers, looking to give agency and security to older adult NPs—both those experiencing memory loss and those charged with overseeing them—without inviting other harms. This problem grows ever more urgent with cybersecurity threats on the rise [21].

2.3. Sociotechnical issues and support for memory loss

This section highlights what we know from the literature about memory concern and technology. Individuals with (un)diagnosed memory loss may be uniquely susceptible to threats because of diminished cognitive abilities that leave them less likely to detect scams and less able to regulate their financial or social activities [26]. Ultimately, oversight may be left to partners who must protect the other from phishing scams and unwise or duplicative purchases [29, 36]. This can create burden and worry for family members and caregivers who feel they are responsible for maintaining the agency of vulnerable partners with agency and their own piece of mind.

While technology could offer a means for NPs to potentially extend support to their partners with memory impairment while living at home, Mahoney et al. pointed out important ethical issues that arise from home monitoring [27]. Their work emphasizes the need for researchers to focus on respect and autonomy for the individual with memory loss, as well as quality of life, but also respect for family caregivers and relationships with caregivers. In so doing, Mahoney et al. usefully highlight the way in which end-users also include family and patient collaborators [21].

Mentis et al. found that in addition to not being able to discern scams and misleading emails, MCI can contribute to embarrassing episodes that cause tension in the family [29]. The solutions that couples formulate in response to online threats vary widely and are not apparently connected to cognitive decline, suggesting that perhaps solutions have more to do with the relationship dynamics than memory loss, or suspected memory loss itself. Couples described a wide range of strategies for managing MCI technology use: never leaving the others side (or "hovering"), to limiting access, to checking their activities once they were done (thus providing autonomy with a "checker"), to taking over for the individual with memory loss when they were no longer able to interact with the system. These strategies reflect not only the cognitive abilities of individuals with memory loss, but also partner dynamics, co-location, caregiver comfort, technological savvy, and tolerance for risk. They reflect a cooperative and constitutive approach that is *sui generis*—too specialized in its character to sit comfortably within a normative frame.

Mentis et al. found that couples are sometimes planning ahead to a point when the individual with MCI is unable to carry on as they once were online, but don't engage in concrete discussions around cybersecurity and access. Although couples express the desire to make shared decisions, in practice, things may happen differently. Mentis et al. report that "shared-decision making was not feasible as there was a lack of suitable options along a spectrum of care" from which the couple could choose, necessitating additional options—not merely "an illusion of choice" [28]. As a consequence, couples were often caught off-guard and prone to taking extreme, disempowering measures when it became clear that one of the partners could no longer manage online [29]. Depending on the couple, however, measures varied substantially from an emphasis on autonomy (wait and see) to an emphasis on safety (abstinence) [28]. The authors describe two ends of the spectrum of safeguarding approaches—on one end, complete oversight and on the other, no intervention at all [29]. Empowerment of those with cognitive challenges means that couples have to find a middle ground that leaves them latitude to plan ahead and gradually transfer knowledge, access, and responsibility. Although flexibility inherently requires work, couples nonetheless do

not want to be limited to a binary option of preserving or removing *complete* access and control. They prefer a degree of nuance that aligns with their relationship dynamics, their experience, and proficiency.

3. Methods

3.1. 'Choice" technology probe for online Safety Settings

We designed a technology probe that embedded hypotheses about choice that were built on prior findings, with the goal of empowering NPs with choice. The probe is realized as a Safety Settings web page, one that provides a spectrum of safeguard features for various online situations that NPs can discuss and choose together. Our ultimate goal is to develop browser plugins that map to these Safety Setting choices to engage NPs in their online activities in a way that ideally safeguards them on terms that are manageable, and which they completely understand. We would not interfere with the collection of data by these services, though.

Informed by the issues already identified by [29, 36] the situations that were presented were for email, Facebook, online banking or money transfer, online shopping, password management, and online browsing. NPs could select settings from any or all of these categories. For each situation, NPs were presented with the option to select a safety setting for two to three actions specified in Table 1.

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

Application/ Situation Category	Online Actions that Entail Risk
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 (PW) 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.

For each action, there was a spectrum of choices provided for the Safety System to enact (see Table 2). This spectrum ranged 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. As the choices moved from no interference to full interference, the choices generally added more security, and in turn one's privacy and autonomy was diminished.

Table 2. Safety Setting Option Levels and Coding for Analysis

Safety Setting Option Level	How Coded in Analysis
Not interfere	1
Record for partner to see later	2
Notify partner	3
Partner review before continuing	4
Review prior to posting (FB only)	5
Deactivate/not allow	6
Couple did not select the situation or unknown	N/A

3.2. Participants

People with some cognitive challenges may ultimately be diagnosed with MCI, but MCI is difficult to diagnosis formally, in part because it is easily confused with natural signs of aging. Our long-term interests are predicated on this uncertainty about cognitive challenges in an older population and thus, we approached recruitment as if cognitive challenges were a concern, not a diagnosis. Specifically, we used self-reported memory concern as a proxy for MCI in determining eligibility. Because deterioration in memory is a pervasive age-related experience and is not necessarily accompanied by a confirmed diagnosis of any kind, our goal, for this research, 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. It ultimately became apparent in the interviews that both partners in all dyads had some memory insecurity or anxiety associated with aging or disease

We recruited a total of 14 individuals (seven NP dyads) to participate in this study. For a dyad to qualify, both partners had to be 65 and older; one or both had to have memory-related concerns (it was not relevant for us to document which person in the screening process); and one or both had to have security concerns online. While one couple was interviewed in-person in their home, the remaining six couples were interviewed using an online meeting tool, GoToMeeting.

The participants were recruited from a marketing panel and, in one case, a continuing care facility with which we have an established relationship. One individual in each dyad was the screened respondent who spoke on behalf of the pair. Assisted living centers were difficult populations from which to recruit couples. We thus turned to a panel to find older adult couples living at home with memory loss. We did not

gather demographic information, as is our practice whenever conducting qualitative research on sensitive topics. Our priority is to ensure that not only will participants remain unidentifiable, that they will have trouble identifying themselves.

In some cases, respondents did not want their memory issues emphasized or even discussed with the other partner while in the interview, so we have taken steps to further conceal identity.

3.3. Study design

The consent form was sent to participants ahead of time for each of them to read and sign. The sessions started with an introduction to the study. NPs were then asked to walk through the system. We used remote access given through GoToMeeting to allow participants to make selections themselves, on the Safety Settings web page, but this only worked once. In all other cases, participants told the investigator what options to select, and the investigator did not speak in order to allow for naturalistic observation.

As NPs made their selection, we asked them to share aloud their thought processes and speak freely with their NP as they decided what settings were most appropriate given their current situation. Given that in previous work, we know that some of the NPs meticulously plan and discuss privacy related issues and settings, this approach was natural.

We followed up each walk-through of the settings mock-up with a brief, semi-structured interview designed to probe usefulness of settings, how NPs might elevate privacy concerns, and how Settings might evolve with the disease progression.

Table 3. Safety Settings Options Chosen for each Situation

	All	Email	FB	Bank	Shop	PW	Browse
Not interfere	31%	21%	57%	29%	29%	7%	29%
Record for partner see later	35%	43%	24%	36%	43%	36%	36%
Notify partner	13%	0%	0%	36%	14%	29%	7%
Partner review	8%	29%	0%	0%	0%	0%	21%
Review prior to posting (FB)	1%	-	5%	-	-	-	-
Deactivate/ not allow	2%	7%	0%	0%	0%	0%	7%
Couple did not select	10%	0%	14%	0%	14%	29%	0%

3.4. Data collection

The walk-through selection of the safety mechanisms and post-interviews were conducted in one couple's home and, for the remainder of our participants, using online GoToMeeting at their convenience. These set ups were audio/video recorded and became part of our study, providing thick descriptions of the sociotechnical dynamic within the NPs. The interviews were completed with one couple at a time. Overall sessions lasted anywhere from one to three hours, depending on how much socializing, technology setup, and logistics (e.g., a NP that was not yet home) were involved. The sessions themselves where NPs engaged with the technology probe only lasted for roughly 20 minutes. These observations were captured on video, audio, and screen captures.

Table 4. Prevalence of Safety Settings Options Chosen for each NP (when NPs made a selection)

	Not interfere	Record for partner	Notify partner	Partner review	Review prior to posting (FB)	Deact./ not allow
NP0	0%	17%	33%	33%	0%	17%
NP1	77%	8%	0%	15%	0%	0%
NP2	0%	75%	25%	0%	0%	0%
NP3	8%	92%	0%	0%	0%	0%
NP4	38%	62%	0%	0%	0%	0%
NP5	23%	0%	54%	8%	8%	8%
NP6	82%	0%	0%	18%	0%	0%

3.5. Data analysis part I

The analysis of the resulting audio/video and screen captures was conducted in two stages. The first stage of analysis was to describe the types of options that were chosen when couples were presented with a full spectrum of choice. We did this in two ways: first, we counted the occurrence of a selection for each option in each context; second, we counted the occurrence of each selection for each option for each NP.

Couples had a total of 13 choices to make, as detailed in Table 1—two per setting (email, banking, shopping, password management, and browsing) with the exception of Facebook, which had three—for a total of 91 potential choices, including no choice at all or N/A. We report on choices NPs made as an aggregate number or percentage of these choices across total situations (out of 91 options) and within situations (out of 14 options, or 21 options for Facebook) (Table 3) and by couples (out of 6-13 choices per couple—

depending on how many settings options they provided an answer for) across situations (Table 4). All of our couples used Facebook, but some do note differences in use among them; and one couple, NP0, did not choose to select Safety Settings for Facebook. NP0 also did not choose to select Safety Setting for online shopping or password management, resulting in them only making 6 choices. NP6 did not choose to have Safety Settings for password management, resulting in only 11 choices. This resulted in 82 total choices being made by couples if N/As are not included. These results merely represent a description of our participants' choices and are not meant to invite statistical inference.

3.6. Data analysis part II

The second stage of analysis was to explain *why* the participants made the choices they made during the study. To answer this question, we used a qualitative approach and first transcribed the discussion the NPs had during the study as well as the post-study interviews. We used a thematic approach to analyze the transcribed data [7]. This approach provided us with the ability to move beyond surface level similarities to salient themes. The analysis focused on the way in which NPs interpreted and made choices around cybersecurity Safety Settings and the way in which sociotechnical roles, concern for autonomy (and its fluidity), and context and experience shaped choice. Our findings organize these themes around the concept of choice, specifically as it relates to protecting shared assets (more surveillance), social activities (less surveillance), fluidity of roles which might mean that they need mutual oversite of sensitive areas or just the option to adjust settings if things change. The analysis was primarily conducted by the first author, who wrote memos from audio/video recordings of the sessions and sorted these findings and transcripts into themes. These were continually presented to the other authors for review and discussion.

Our presence in this process from recruitment through interviewing takes the form of both silent observer and disrupter, but neither role can be deemed unobtrusive, as we will show. We did not seek out generalizability so much as an encounter with choices and how NPs understand and negotiate them, taking into account highly idiosyncratic and personal/private matters related to memory loss and broader uncertainty around aging.

4. Findings

4.1. Choices made

NPs most frequently choose Safety Settings where they could record their activities for their NP to see later, 32 out of 91 choices, followed by no interference, 28 out of 91 choices (see Table 3). Variations in their choice of Safety Setting stringency often reflect the context, whether they had more or less concerns about safety or were (sometimes regardless of memory loss) worried about being the target for scams in ways that required mutual oversite.

Email elicits the most stringent settings (5 out 14 selections required partner review or deactivate/not allow) followed by banking (5 out of 14 choices were notify partner) password management (4 out of 14 choices were notify partner), browsing (5 out of 14 with 1 choosing notify partner, 3 choosing partner review, and 1 choosing to deactivate altogether). The other categories (shopping and Facebook) tend to elicit less strict Safety Setting selections, erring (slightly) more often on the side of no interference or record for later. These were situations that were more social (more individual), and thus, more interlaced with autonomy, whereas the other settings tended to involve more shared assets and thus, shared safety.

Table 3 shows the safety selection by feature category within each situation. There are only a few exceptions where NPs make selections that were more stringent for a certain feature: opening email attachments (as opposed to opening links), commenting on Facebook posts or accepting/rejecting friend requests (as opposed to liking a post), transferring money (as opposed to viewing one's accounts), clicking on links while browsing (as opposed to searching). Password management Safety Settings choices are the least stringent when it came to changing passwords on the computer (as opposed to on sites).

Most often NPs choose to record activities for them self or the other partner to see later, but many still choose the setting "no interference." When NPs make these selections, it is frequently described as providing a log for *both* them and their partner.

4.2 Seeing from the other's perspective and memory loss uncertainty

Couples' choices tend to reflect awareness that memory loss could affect either partner, and this awareness inspires a dual perspective on Safety Settings, also enabling them to take account of the needs and the styles of each, and the challenges of co-managing the ramifications of memory loss.

NP2-2 imagines the breadth of those ramifications:

> NP2-2: It could be your own memory, 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 … and it could go fast maybe me more than [partner] because every indication I could have a problem. I do so I don't mind, you know it's less onerous for him as long as we just agree we're going to have some checks and balances.

Couples appreciate that they have the flexibility to choose settings as the memory of *either* one declines. They emphasize that collaborative oversight gives them the

opportunity to mutually manage risk but also that, for now, autonomy is essential ("the ball is in her court").

> NP1-1: If we were feeling that one had more memory loss than what we are initial thinking, which she will get, and I will too … She still can remember … We still have to have the safety because we are among each other to do it.
> NP1-2: I forgot today.
> NP1-1: 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.

Couples also express uncertainty about progression, and speculate that settings might need to change in a year, or five, or ten years:

> NP3-2: Yes. it could be 5 years it could be 10 years and we…
> NP3-1: It could be tomorrow we don't know…

> NP4-1: Yeah, because like say, I think that our circumstances are different right now. I think we would answer them differently maybe in a year so.

This way of thinking of memory loss as possibly affecting both of them and having an uncertain timeline supports, as we will show, a collaborative way of thinking about their cybersecurity as a shared challenge.

In the sections that follow, we present the qualitative analysis from our observations and interviews, describing how our participants viewed each level of choice.

4.3. Not interfere

The choice to "not interfere" was the second most frequently made (28 out of 91 choices) after 'record for partner to see later' (32 out of 91 choices). This was particularly the case in the context of social activities (like Facebook 12 out of 21 choices) and when the partner perceived their choice would encroach on the other's autonomy—e.g., with regards to shopping or browsing as well as banking (4 out of 14 choices in all cases).

In the context of social interaction, a common response to this setting is that only one of the NPs actually uses Facebook, even if they both have it. Those that do choose to have Safety Settings for Facebook, largely choose "no interference," agreeing that social activities is the other's private business.

Facebook was the only application where NPs were given the additional choice to have one partner review the activities prior to posting. This was not a top choice because couples do not want to infringe on the others social autonomy:

> NP1-1: Like what you like.
> NP1-2: Do not interfere.

This couple communicates a sentiment widely shared: that these settings were meant to provide security but not "clip their wings." There they draw the line.

Browsing is not an application NPs necessarily want any Safety Settings for, though they indicate it as an application or situation for which they want to set Safety Settings, perhaps because they assume it is something that they always do and thus seems obvious or necessary to discuss.

Couples want to ensure autonomy where there no shared assets. For example, for NP1, having accounts they did not share makes them comfortable with no interference:

> NP1-1. Separate accounts. Not interfere.

This couple, like others, is sensitive about preserving autonomy where it already exists. Along those lines, one couple considers only that "review" is necessary and otherwise "not interfere."

> NP3-1 The only way I would want this to work is if I need her to review it, otherwise "not interfere." Does that make sense? I don't know if that's an option.
> Interviewer: Did any of the options look to you as if the partner would have the opportunity to review it in a way that you would be happy with? For instance [reads options …].
> NP3-1: What does "deactivate all links" mean. [inaudible] Thank you, I want to know what they're looking for?
> Interviewer: This would make it so a person could not click on links in email.
> NP3-1: Okay. I don't think I'd want that. I guess, "Not interfere."

NPs frequently toggle between "not interfere" and "review for later," but often side with the choice that gave more autonomy if possible.

4.4. Record for partner to see later

Most often NPs choose to have their activities "recorded for their partner to see later" (32 out of 91 choices), and this applied across situations. NP6 communicates that they are not worried about memory loss, but rather malicious links that could be inadvertently selected for reasons having to do with the other's technical knowledge and past experience with scams in email and Facebook. Recall that NP3 wanted only to "review activities" when it made sense in context. Later, they refine their selection saying that what they wanted is to "record their activities for their partner to see later" (for both links and attachments) with the expectation that it will serve *their* memory (not necessarily for their partner's oversight, though some NPs suggest that is the ultimate expectation). For instance, in the following example, NP3 moves onto the next option setting and in the course of making this selection goes back to the prior selection to change it from "not interfere" to "record":

> NP3-1: Okay, okay. Now I understand the concept. If that is the case, then I would want to have a log of everything that I did so go back to the previous one [previous option setting question]. Okay. Yeah, I'd like to "record all the links I click on for your partner to see later." I'd say that one. In other words, I would have a log to refresh my memory because that's what I need.

This same couple selects the setting to record what their partner posted on Facebook for the other to see, later saying that they did not put personal things on Facebook but wanted it just in case.

> NP3-1: Well she does Facebook. I don't do Facebook. So.
> NP3-2: I guess record all Facebook comments for your partner to see later, is the only thing. I don't use it where I put anything personal on it, but just in case.

For this couple, concern that either of them could lose their memory counts as a reason to have some record for either or both of them—a decision that serves their sociotechnical habits well because each partner has different methods of organization:

> NP3-2: 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.

Online banking and shopping are frequently recorded for one's partner to review later because, for most, it is not of great concern. NP2 approaches it with a mixture of humor and seriousness, allowing for the possibility to need a stricter setting later:

> NP2-2: I would say "record all the places that your credit card is going." Number 2. Otherwise or "immediately notify of the sites where you can enter your credit card number." But that's gonna slow you down.
> NP2-1: Yeah because you're gonna wanna buy stuff without having to talk.
> NP2-2: Well, I'm just concerned you're gonna reach a point where you are spending on what you want necessarily not that you need it. Okay?
> NP2-1: This means I can't surprise you with any presents.
> NP2-2: Oh boy I need to rethink that.
> NP2-1: Which one?
> NP2-2: How about "immediately notify your partner of purchase amount or record all purchase amounts for your partner to see later."
> NP2-1: Which one?
> NP2-2: You can do two if you want, maybe…
> NP2-1: Why don't you just do 1?
> NP2-2: You can do choice number 2 ….
> NP2-1: Okay.

At one point, NP2-2 again expresses concerns that their partner could buy things they wanted but did not need. Pointing out that their partner has bought a car once online, NP2 still selects "record" and not the more stringent option:

> NP2-2: I worry about… my worry is you might go buy a car at some point, and yes, he has bought a car on the Internet just once.

This couple's worries were clearly linked to memory loss and an impending sense of changing roles. Perhaps, as a result, they participated in a lot of back-and-forth in which they debated the option that they thought was most fitting, reluctant to give up autonomy. In these cases, options provided along a spectrum allowed for a negotiation space and outright discussion of what some of the potential incidents might be on the horizon.

4.5. Notify partner

The choice to keep NPs aware of what the other was doing in real time is much less often selected (12 out of 91 choices) but tends to come up where there were concerns about "shared assets," which included both banking and passwords. The function of these notifications was to be aware of activity for security and potential intervention (in the case of banking) and to stay abreast of changes, as well as for their own recall (in the case of passwords). In that sense, notification choice served different purposes, one being more about security from cognitive challenges and malicious activity, and the other more about memory management, respectively.

Several NPs choose to have their partner notified of online banking activity. Notably, NP3 remarks that these settings might become more stringent, in one case, citing worrisome incidences with other members of the family who have also experienced memory loss:

> NP3-1: Yeah. Banking account. Same thing: keep a log of what I am doing to help me remember for later. I guess it depends on the extensiveness of the mental disease that you are having as far as memory. If you want to be notified immediately or later. Right now, I would need it later.
> NP3-2: But this would be something that could be put in place if things changed. His mother suffered from a lot of memory issues and she denied she had a lot of it. And I would want this.

Again, we see a lot of discussion addressing concern about cognitive challenges that could change dynamics. This sentiment was illustrated by NP3 and also echoed by NP2; the only difference is the stringency of settings they finally settled on.

Password management also frequently prompts selection of "notifying" one's partner, mostly because NPs relate that they often forget their passwords and are constantly resetting them; and they consider passwords to be a shared asset. Not only did they want their partner to be able to see what they chose as their new password, they also want to be reminded of the password themselves. NP2-2 wants to notify their partner of a change because they feel that they would want that for them self, even if they did not have memory issues:

> NP2-2: Do you think you need notification when they change because you change your passwords frequently. Well you do when you can't remember you changed…
> NP2-1: Well this is for you to know
> NP2-2: OK
> NP2-1: Not for me to know
> NP2-2: Right, or that I can help you with passwords…

NP2-1: Focus on your own
[Both Laughing]
NP2-1: I might want notifications on mine
NP2-2: Do you wanna go back [to choosing option notify partner from record for partner to see later]
NP2-1: Yeah. We can click the third one

This exchange between NP1 and NP2 shows how this tool was not only about safeguards for memory loss but everyday memory issues associated with life online—and possibly, though not certainly, aging. It highlights how assets are a kind of shared concern that can overlap with autonomy.

Couples feel that choice of notifying partner was particularly important around issues of shared assets. They wanted to be able to enforce a kind of mild surveillance to ensure security—not just from forgetfulness but also bad actors, who, according to one couple, were sometimes in their own family. Another couple points out that with anything related to money or passwords, they are more leery:

NP3-1: If it's, if it's related to money I would say yes, depending upon, you know, how bad we are … We keep passwords the same thing. It's like giving the key to your house. you know somebody gets a gift card to a website they can do whatever they want.

To demonstrate the importance of the choice to notify partner as a way of keeping an eye on shared assets and providing protection from outside actors, one couple would like notification to alert them when their grandson is browsing and downloading a file:

NP5-1: My grandson is five. He gets on the computer. I would want [Safety Settings] to immediately notify you are downloading a file ... He uses it for school, to do homework stuff.

The idea of protecting yourself against family is, for NP5, made more salient by things they had heard from friends, as well as experiences they had had with family.

In general, we found that the choice to notify partner is critical in the context of shared assets, where the risks make surveillance much more acceptable.

4.6. Partner review

On occasion, NPs choose to have their partner review at the moment of action and approve or deny (7 out of 91). Desire for intervention is most pronounced with email, where there is a sense of being targeted and an accompanying concern about clicking on malicious links. As NP6-1 describes, she is worried, even now, about that vulnerability, and her partner's ability to assess what is malign, independent of memory issues.

NP6-1: I trust him but I don't trust other people on the computer and the different things they may do. If I send him something through an email … and I'll put some kind of little note where he'll know it's something. Where if I didn't, I'm wondering, "would he just click it?" So, I don't know all the scenarios, so that's where I would say that.

This couple mentions that they have talked about not clicking on links sent by their family members out of fear that they are malicious and have developed a practice of mutually alerting so that the person with more computer knowledge can assess the link. The ability to imagine that things could get worse for either member of the pair leads couples to appreciate the option of having a partner review. Still, some expressed concerns about the potential for such an option to become invasive and also burdensome.

4.7. Deactivate

Deactivation or allowance of activity was presented as disabling those links not on a preapproved safe list or disabling the activity altogether, depending on the setting. Only two couples chose to have settings deactivated, for email attachments and for browsing, out of concern that by the time their partner clicks on it, it will be too late. This was simply not a popular choice and not even one that couples discussed using as they imagined more stringent settings down the road.

NP5-1 chooses "deactivate links" in search on a list that they were able to curate because they feel that this safety measure protects *both of them* from malicious attack, not because of memory loss.

NP5-1: I would only put like places that … I normally browse.

NP5 was concerned about the need to adjust settings to accommodate memory loss but, these decisions tended to be between "no interference" and "review" or "notification," and not "deactivation."

The choice of deactivation is a last resort, one that couples consider only where they fear they may become helpless—not necessarily as a result of memory loss but rather, due to the activities of bad actors. We posit that, given all the choices couples do have, the prospect of deactivation seems remote.

5. Discussion

NPs like the option of being able to notify their partners, particularly in the realm of shared assets. Because they imagined themselves potentially in the same role, and because the course of memory loss is recognized as so uncertain, the concept of shared privacy has some appeal.

This runs in contrast to the idea that couples are managing their privacy settings individually as most systems assume. The choices couples make reflect joint ownership of the problem as well as respect for autonomy by (paradoxically) embracing uncertainty, a "see-as-we-go" attitude expressed by all of our couples.

5.1. Choice reinforces autonomy

Having flexibility of choice fits NPs well in that it allows them to begin with a light touch and then introduce more safety as they sense decline. Even measures like keeping a

record are quickly recognized as offering mutual benefit—the idea of providing a history for their own convenience and later, an oversight resource that is available to their partner. NPs often think about an indeterminate, future time when either of them might handle their finances in an unsafe way. This led them to want the ability to be aware of what the other was doing, and also provide access at a later date (maybe five to ten years, they could not be sure) to a family member who might need to supervise both of them.

Overall, preserving autonomy was paramount. NPs consider what these choices might mean for the person with oversight, as well as for the person in need of oversight. Their ability to pivot in these ways, between present and future, self and partner, reflected their grasp of mutual vulnerabilities.

We plan to test the adaptive nature of this design by allowing couples to adopt these Safety Settings over an extended study. Our future study design will prompt couples to reflect on Safety Setting changes to capture whether they are motivated to adjust their settings over time in response to experiences of risk [22] or memory decline [34].

Future designs will iterate on ways to make the option to adjust Safety Settings apparent. We will be interested to see if those design changes influence Safety Setting choices, and how the pace and rate of adjustment relates to breaches in security, changes in cognitive status, and even to changes in relationship dynamic as couples adapt to progression. Because participants themselves could not reasonably project the future, or even imagine themselves capable of doing so, the triggers for adjustment remain unclear.

5.2. Choice supports *social autonomy*

Choice allowed couples to extend continuing autonomy to their partners in social realms, where they deem latitude important. Facebook tended to be designated for nonintervention based on what couples explained was a desire to extend freedom to socialize. These decisions could be the result of couples' failure to fully appreciate all the ways in which Facebook invites risks. Note that we did not provide an extensive list of Facebook activities which might be considered more risky (e.g., posting or clicking on a link). Future design iterations should include a more concrete explication of these activities and risks.

5.3. Choice supports *shared assets* and sociotechnical idiosyncrasies

We found the logs and more overt forms of review and notification surveillance provided a way to personally retrace steps or intervene around shared assets. For both NPs, these more stringent settings provided insight into what was done that solved current struggles with maintaining shared assets. In other words, they served the current dynamic and provided a buffer for all parties.

5.4. Choice that embraces *uncertainty* supports autonomy for partner and self ("It could be me")

Simply by introducing choices, the couples were able to customize each safety setting in a way that preserves more autonomy for both the partner with greater memory concern and the one with less. Those roles were acknowledged to be *uncertain* at the beginning. Thus, the "record" option, in particular, was seen as allowing a person with memory loss to access their own logs (enacting a sort of personal surveillance) and also permitting the person with less memory concern to eventually review them. The fact that these roles could potentially be reversed in the event that health circumstances change (e.g., if one suddenly declined faster) made them more sensitive to the need for a system that was adaptive and, and sensitive to each other's feelings and requirements. For this reason, the wording of the system could be oriented towards more cooperative oversight, rather than for later review by just one partner.

We contend that this embrace of *uncertainty* shapes choice and broader, long-term thinking about the utility and place of this system. Even NPs who had identified one partner as suffering from more decline acknowledged that they could suddenly be the ones to require more assistance. We interpreted this admission as both acknowledgment of the fragility and uncertainty and unpredictability of memory loss, and also maybe a feeling that the individual at greater risk might skirt the supposed prognosis. Nothing is certain, which is why collaborative and adaptive approaches seem all the more appropriate.

Because NPs are open to the idea that memory loss is part of aging (even if it may overtake one of them more quickly, or dramatically) they are quick to offer that they would like to include a family member (or even a caregiver) in this system. Although the potential for caregivers or even family to take advantage of this access does come up, it is not a major concern. At the same time, as NP5 pointed out, family can be the source of security threats.

Future design iterations will explore ways to foster self-surveillance and make record-keeping less obtrusive and burdensome to the partner. These choices might still include latent monitoring and alerts that allow the other partner to retain oversight over those records. Because partners are open to the possibility that their roles might change, we will need to carefully consider how we articulate or impose them.

5.5. Choice means more risk

Even if they worry about shared assets, NPs are prone to accept more risk out of respect for partner autonomy and in deference to changing circumstances and roles. This tendency also coincided with a desire not to disclose memory concern or to accept that "it could be me." Because we did not seek out couples with a diagnosis, we had to be

comfortable with ambiguity in our approach. Future design iterations must be attuned to this ambiguity; the sensitive nature of disclosure; and the evolving nature of cognitive decline in relationship to risk.

When designing future iterations, we will look to collaborative service provider models for inspiration and to help frame, in particular, our understanding of shared risk in relationship to autonomy.

6. Conclusions

NPs facing memory loss with cybersecurity concerns think things through as a unit facing very certain health-related ambiguity. They confront the opacity of their situation as a team (one said "as a game"); while they have collaborated in life and in partnership, they are entering a new phase of sociotechnical collaboration around the others or one another's memory decline. We have looked at how NPs work through these issues, finding that relationship dynamics, technological habits, idiosyncrasies, and shared concern, or ability to imagine their own memory decline shapes decisions around cybersecurity Safety Settings. Our findings suggest that NPs need a dynamic system that adapts to their memory concerns (or progression) and anticipates fluidity of roles and the realization that they are not only collaborating in shared preservation of their safety but in a dynamic system that could change. The key component of negotiation was empathy—belief that they are a unit with shared stake and that the roles could be reversed at any time.

NPs are worried about cybersecurity independent of memory issues, like links in email, identity theft and impersonation on social media, social engineering in email, and family members without impulse control. It can therefore be difficult to parse concerns related to memory loss from those inspired by their own experience of risk and threat or media and advocacy group exposure (e.g., AARP).

6.1 Limitations

Our experimental design is limited in several notable ways. First, although we engaged in naturalistic observation, we nevertheless required that couples engage in negotiations out loud with us. Future research will involve diary studies over a longer period to allow participants to negotiate and adjust settings in their natural environment, at their own pace, and as circumstances change. Second, the scenarios we provide, particularly for Facebook, were limited. There are other activities on Facebook that one could engage in that may, in fact, be riskier. Third, despite intensive recruiting efforts, our study involved a limited sample drawn from an online panel, and thus technological adept enough to participate in online surveys, although the technological bar for online panel participation is relatively low. Finally, our study design looked exclusively at couples, and while these findings lend support to the view that cybersecurity is a joint (rather than individual) burden, we will need to conduct complementary research that engages partners as individuals, outside a dyadic context, for a different sightline.

ACKNOWLEDGMENTS

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

REFERENCES

[1] Acquisti, A. 2009. Nudging Privacy: The Behavioral Economics of Personal Information. *IEEE Security Privacy*. 7, 6 (Nov. 2009), 82–85.

[2] Acquisti, A., Brandimarte, L. and Loewenstein, G. 2015. Privacy and human behavior in the age of information. *Science*. 347, (Jan. 2015), 509–514.

[3] Altman, I. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. Brooks/Cole.

[4] Apple and Google's tough new location privacy controls are working: 2020. *https://www.fastcompany.com/90454921/apple-and-googles-tough-new-location-privacy-controls-are-working*. Accessed: 2020-02-13.

[5] Baruh, L. and Popescu, M. 2015. Big data analytics and the limits of privacy self-management: *New Media & Society*. (Nov. 2015).

[6] Batchelor, R., Bobrowicz, A., Mackenzie, R. and Milne, A. 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.

[7] Braun, V. and Clarke, V. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology*. 3, 2 (2006), 77–101.

[8] Brooke, A. and Raine, L. 2019. Key takeaways on Americans' views about privacy, surveillance and data-sharing. *Pew Research Center*.

[9] Caregiving for Person with Alzheimer's Disease or a related Dementia | Alzheimer's Disease and Healthy Aging | CDC: 2019. *https://www.cdc.gov/aging/caregiving/alzheimer.htm*. Accessed: 2020-05-20.

[10] Cate, F.H. 2006. *The Failure of Fair Information Practice Principles*. Technical Report #ID 1156972. Social Science Research Network.

[11] Cate, F.H. 2010. The Limits of Notice and Choice. *IEEE Security Privacy*. 8, 2 (Mar. 2010), 59–62.

[12] Cavoukian, A. 2009. *Privacy by Design - The 7 Foundational Principles*. Information and privacy commissioner of Ontario, Canada, 5.

[13] Dementia cases set to triple by 2050 but still largely ignored: *https://www.who.int/mediacentre/news/releases/2012/dementia_20120411/en/*. Accessed: 2019-10-04.

[14] Facts and Figures: *https://alz.org/alzheimers-dementia/facts-figures*. Accessed: 2019-10-03.

[15] Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T. and Dell, N. 2018. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. (2018), 1–13.

[16] Ghosh, A.K., Badillo-Urquiola, K., Guha, S., LaViola Jr, J.J. and Wisniewski, P.J. 2018. Safety vs. Surveillance: What Children Have to Say About Mobile Apps for Parental Control. *Proceedings of the 2018 CHI Conference on Human*

Factors in Computing Systems (New York, NY, USA, 2018), 124:1–124:14.
[17] Grassi, P.A., Garcia, M.E. and Fenton, J.L. 2017. Digital Identity Guidelines. (Jun. 2017).
[18] Gray, C.M., Kou, Y., Battles, B., Hoggatt, J. and Toombs, A.L. 2018. The Dark (Patterns) Side of UX Design. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada, Apr. 2018), 1–14.
[19] Hartzog, W. 2017. The Inadequate, Invaluable Fair Information Practices. *76 Maryland Law Review 952; Northeastern University School of Law Research Paper No. 301-2017*. (2017).
[20] Hull, G. 2015. Successful Failure: What Foucault Can Teach Us About Privacy Self-Management in a World of Facebook and Big Data. *Ethics and Information Technology*. 17, 2 (2015), 89–101.
[21] Identity Theft Soared to a Record High in 2017: 2018. *http://www.aarp.org/money/scams-fraud/info-2018/id-theft-fraud-fd.html*. Accessed: 2019-12-24.
[22] Kang, R., Brown, S. and Kiesler, S. 2013. Why Do People Seek Anonymity on the Internet?: Informing Policy and Design. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2013), 2657–2666.
[23] Kaye, J. "Jofish" 2011. Self-reported password sharing strategies. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Vancouver, BC, Canada, May 2011), 2619–2622.
[24] Kokolakis, S. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*. 64, (Jan. 2017), 122–134.
[25] Lazar, A., Edasis, C. and Piper, A.M. 2017. Supporting People with Dementia in Digital Social Sharing. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2017), 2149–2162.
[26] Lorenzen-Huber, L., Boutain, M., Camp, L.J., Shankar, K. and Connelly, K.H. 2011. Privacy, Technology, and Aging: A Proposed Framework. *Ageing International*. 36, 2 (Jun. 2011), 232–252.
[27] Mahoney, D., Purtilo, R., Webbe, F., Alwan, M., Bharucha, A., Adlam, T., Jimison, H., Turner, B. and Becker, S. 2007. In-home monitoring of persons with dementia: Ethical guidelines for technology research and development. *Alzheimer's & dementia : the journal of the Alzheimer's Association*. 3, (Aug. 2007), 217–26.
[28] Mentis, H.M., Madjaroff, G., Massey, A. and Trendafilova, Z. In submission. The Illusion of Choice in Discussing Cybersecurity Safeguards Between Older Adults with Mild Cognitive Impairment and Their Caregivers. *Proceedings of the ACM Conference on Computer-Supported Cooperative Work & Social Computing* (In submission).
[29] Mentis, H.M., Madjaroff, G. and Massey, A.K. 2019. Upside and Downside Risk in Online Security for Older Adults with Mild Cognitive Impairment. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2019), 343:1–343:13.
[30] Mild cognitive impairment - Symptoms and causes: *https://www.mayoclinic.org/diseases-conditions/mild-cognitive-impairment/symptoms-causes/syc-20354578*.
[31] Morgan, S. 2018. Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021. *Cybercrime Magazine*.
[32] Nissenbaum, H. 2010. *Privacy in context: technology, policy, and the integrity of social life*. Stanford Law Books.
[33] Parental monitoring apps: How do they differ from stalkerware? 2019. *https://blog.malwarebytes.com/stalkerware/2019/07/parental-monitoring-apps-how-do-they-differ-from-stalkerware/*. Accessed: 2019-12-17.
[34] Patil, S. and Lai, J. 2005. Who Gets to Know What when: Configuring Privacy Permissions in an Awareness Application. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2005), 101–110.
[35] Petronio, S.S. 2002. *Boundaries of privacy: dialectics of disclosure*. State University of New York Press.
[36] Piper, A.M., Cornejo, R., Hurwitz, L. and Unumb, C. 2016. Technological Caregiving: Supporting Online Activity for Adults with Cognitive Impairments. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16* (Santa Clara, California, USA, 2016), 5311–5323.
[37] Sachdev, P.S. et al. 2015. The Prevalence of Mild Cognitive Impairment in Diverse Geographical and Ethnocultural Regions: The COSMIC Collaboration. *PLoS ONE*. 10, 11 (Nov. 2015).
[38] Schaar, P. 2010. Privacy by Design. *Identity in the Information Society*. 3, 2 (Aug. 2010), 267–274. DOI:https://doi.org/10.1007/s12394-010-0055-x.
[39] Singh, S., Cabraal, A., Demosthenous, C., Astbrink, G. and Furlong, M. 2007. Password sharing: implications for security design based on social practice. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (San Jose, California, USA, Apr. 2007), 895–904.
[40] Spiekermann, S. and Cranor, L.F. 2009. Engineering Privacy. *IEEE Transactions on Software Engineering*. 35, 1 (Jan. 2009), 67–82. DOI:https://doi.org/10.1109/TSE.2008.88.
[41] Tejada-Vera, B. 2013. Mortality from Alzheimer's disease in the United States: data for 2000 and 2010. *NCHS data brief*. 116 (Mar. 2013), 1–8.
[42] Tene, O. 2013. Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws. *Ohio State Law Journal*. 74, 6 (2013), 1217–1262.
[43] The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry: 2019. *https://citizenlab.ca/2019/06/the-predator-in-your-pocket-a-multidisciplinary-assessment-of-the-stalkerware-application-industry/*. Accessed: 2019-12-24.
[44] What Is Mild Cognitive Impairment? *https://www.nia.nih.gov/health/what-mild-cognitive-impairment*. Accessed: 2019-10-03.
[45] Xu, B., Chang, P., Welker, C.L., Bazarova, N.N. and Cosley, D. 2016. Automatic Archiving Versus Default Deletion: What Snapchat Tells Us About Ephemerality in Design. *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing* (New York, NY, USA, 2016), 1662–1675.
[46] Zuboff, S. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.