Using a Participatory Activities Toolkit to Elicit Privacy Expectations of Adaptive Assistive Technologies

Foad Hamidi, Kellie Poneres, Aaron Massey
University of Maryland, Baltimore County (UMBC)
Baltimore, MD, USA
{foadhamidi, kellie5, akmassey}@umbc.edu

Amy Hurst
New York University (NYU)
New York, New York, USA
amyhurst@nyu.edu (

ABSTRACT

Individuals whose abilities change over time can benefit from assistive technologies that can detect and adapt to their current needs. While these Adaptive Assistive Technologies (AATs) offer exciting opportunities, their use presents an often-overlooked privacy tradeoff between usability and disclosing ability data. To explore this tradeoff from end-user perspectives, we developed a participatory activities toolkit comprised of tangible low-fidelity physical cards, charts, and two software AAT prototypes. We used the kit in interviews with six older adults who experience pointing and typing difficulties when accessing the Internet. Participants had conflicting views about AATs collecting their data, and strong preferences about what data should be collected, how should it be used, and who should have access to it. The contributions of this paper are twofold: (1) we describe a novel approach to elicit detailed end-user privacy preferences and expectations, and (2) we provide insights from representative users of AATs towards their privacy.

CCS CONCEPTS

Human-centered computing ~ Accessibility design and evaluation methods

KEYWORDS

Assistive Technology; Adaptive Systems; Privacy; Participatory Toolkit; Low-fi Elicitation Tools

ACM Reference format:

Foad Hamidi, Kellie Poneres, Aaron Massey, and Amy Hurst. 2019. Using a Participatory Activities Toolkit to Elicit Privacy Expectations of Adaptive Assistive Technologies. In *Proceedings of the 17th International Web for All Conference (W4A'20). ACM, New York, NY, USA, 10 pages.* https://doi.org/10.1145/3371300.3383336

W4A '20, April 20–21, 2020, Taipei, Taiwan

ACM ISBN 978-1-4503-7056-1/20/04…$15.00
https://doi.org/10.1145/3371300.3383336

1 Introduction

There is a growing concern from disability activists and accessibility researchers about privacy threats posed by technologies that collect and track user data [18] [48] [63]. These concerns include efforts by developers to automatically detect accessibility settings on users' devices (e.g., detecting the use of screen readers) to adapt content. Despite a goal of improving user experience, linking user data to a health condition or disability, often without informing the user, poses serious privacy threats; threats exacerbated by the ongoing trade of users' data between third party companies [48]. Therefore, there is an urgent need to better understand end-user perspectives on the privacy tradeoffs of these technologies.

Adaptive Assistive Technologies (AATs) monitor a user's current and past performance and adapt their functionality accordingly [36], [38], [45]. They are particularly promising for users whose abilities change throughout the day due to medication, fatigue, stress, or a medical condition. For example, to best help an individual with a hand tremor (caused by Essential Tremors or Parkinson's Disease) use a mouse, software must constantly observe their mouse use and model the severity of the tremor, and mouse movements. An AAT can then use this data to track when the user experiences severe pointing problems and employ techniques to mitigate them.

While AATs offer exciting accessibility and usability opportunities, their use requires the collection of potentially sensitive data regarding a user's ability, efficiency, or accuracy. Users who rely on these tools for education, communication, and employment may be unaware of their potential to disclose private information about their ability, usage habits, or performance. For example, disclosure of early-stage Parkinson's Disease to an employer, insurance company, or advertising company could have significant implications. Unfortunately, assumed legal protections may be inadequate to protect this information. For example, the U.S. Health Insurance Portability and Accountability Act (HIPAA) only applies to health care providers and associated business entities, not employers [53].

In this paper, we first present a participatory activities toolkit for eliciting detailed privacy preferences and expectations of AATs (Figure 1). We then present privacy insights about the privacy tradeoffs of using AATs gathered with the toolkit from six older adults who experience computer access challenges. These

contributions complement ongoing research on informing the design of emerging technologies with end-user privacy perspectives [56], [57] and demonstrate how participatory hands-on approaches can facilitate conversations on privacy with non-technical participants. Our toolkit can be extended to understand perspectives towards other technologies.

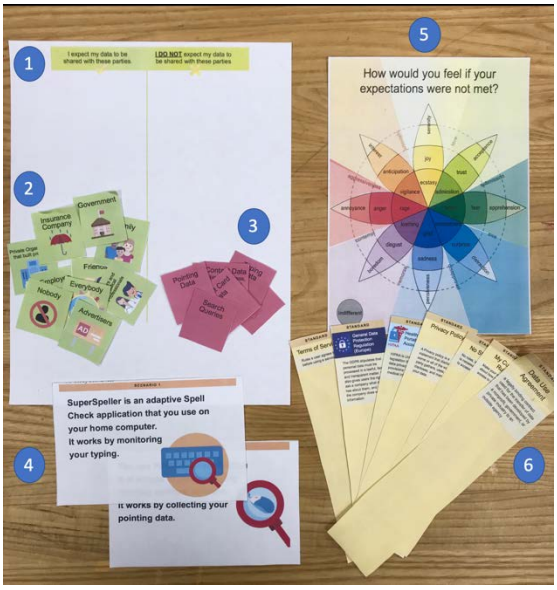

Figure 1. Overview of materials developed for the Participatory Activities Toolkit: (1) Expectations Chart, (2) Third Party Cards, (3) Data Type Cards, (4) Scenario Cards, (5) Wheel of Emotion, and (6) Privacy Standard Strips.

2 Related Work

The importance of including diverse user perspectives towards the design of emerging technologies is increasingly recognized in the Privacy and Security research communities [56], [57]. For example, the Inclusive Privacy and Security initiative [55] has been organizing community-building workshops and online initiatives to bring together researchers and practitioners who work with diverse user populations [62] with the goal of "designing security and privacy mechanisms that are inclusive of people with various characteristics, abilities, needs and values [56]." Within the accessibility and assistive technology research and practice communities, the importance of investigating the privacy implications of emerging technologies is also recognized (e.g., [18], [48][63]). We contribute to this space by proposing a novel method to elicit input from non-technical participants and by sharing findings collected using our method from older adults who experience difficulties accessing the Internet. We next summarize research on end-user perspectives on the privacy of adaptive technologies and methods for eliciting them.

2.1 End-User Perspectives towards Adaptive Technologies

A growing body of research on end-user perceptions and attitudes towards privacy tradeoffs of adaptive and personalized applications has emerged in the last few decades (e.g., [2], [5], [24], [50], [64]). Many of these projects focus on online marketing [2], [50], Internet-of-Things (IoT) and wearable applications for health [15], [64]. Several studies reported users expressed feelings of "creepiness" and "panic" when they learned about how their data could be used outside of the original context of an application use [2], [50]. For example, Angulo and colleagues identified 18 scenarios of privacy-related panic through interviews with 14 participants. Cases of account hijacking and personal data "leakage" were among the most memorable panic scenarios for participants [2]. Researchers have identified a mismatch between users' mental models and how personal data is actually collected and used as a factor that can lead to unpleasant surprise and discomfort when users are informed about discrepancies between their expectations and the actual privacy characteristics of an application [5], [15], [24], [64]. For example, most Americans are unaware that companies use automated systems without human intervention to review job applications, and when informed about the practice, 67% found it at least somewhat worrisome [40].

Providing users with explicit notice of privacy practices and then offering them a choice in their use of the associated tools is the intuitive answer to this general lack of end-user awareness. Referred to as Fair Information Practice Principles (FIPPs), this approach has even been the general guidance offered by regulatory agencies, including the U.S. Federal Trade Commission [12]. Unfortunately, the FIPPs are now recognized to be flawed and have failed to meaningfully address the problems we outlined above [8][23]. Although an amended HIPAA or new regulations like the E.U. General Data Protection Regulation (GDPR) may ameliorate this situation, we believe engineers have an ethical responsibility to understand user expectations and perceptions of the tools they use and adjust their design accordingly [19]. Moreover, fulfilling this ethical responsibility is non-trivial in the design of assistive technologies because view health information as intensely private, whereas others openly share their health-related challenges [19].

To date, few studies have examined the privacy tradeoffs of AATs. Hamidi et al. presented a threat modeling meta-analysis of AATs to categorize possible threats that they can pose to users [18]. The analysis was followed by an interview study with 8 older adults who experience pointing difficulties towards AATs that support their Internet access. While the participants were willing for their pointing data to be collected and used to improve system functionality for themselves and others, they had strong preferences about who should access their data. Participants also described privacy concerns that mapped to all of the privacy threat categories identified in the analysis [18]. The project focused on one type of AAT and did not investigate participants' emotional response towards privacy threats and how they wished to mitigate them.

Other related projects focused on health monitoring and location sensing systems for older adults [34], [54]. For example, McNeill and colleagues conducted interviews with 20 older adults about their privacy concerns with pervasive health-monitoring systems [34]. They found that privacy was valued by their participants and important to their sense of life fulfilment. The authors recommended against ageist approaches that involve gathering

extensive data to monitor older adults' physical and cognitive decline at the expense of their privacy [34]. In the context of dementia care, several projects identified privacy tradeoffs that arose when GPS-enabled devices were used to track of users' location to increase their physical safety [28], [29]. This previous research points to the development of multifaceted strategies that combine technical, legal and social mechanisms to develop "privacy-friendly" personalized systems [26], [30], including IoT systems for people with disabilities [22]. These strategies require methods to incorporate diverse end-user perspectives that inform designers about the sociotechnical issues required to develop and deploy these systems [10], [54], [56].

2.2 Eliciting Non-Technical Privacy Perspectives

Different methods such as interviews [59], [3], [24], surveys [58], and focus groups [31], have been used by researchers to investigate users' mental models and attitudes and perceptions towards privacy. Ray et al., asked 20 older participants to create open-ended drawings that expressed their conceptions of the general concept of "privacy" in both digital and non-digital contexts [44]. This activity was followed by semi-structured interviews where participants elaborated on their drawings. The study revealed participants' privacy concerns, feelings of resignation and fear, and protection strategies. In another study, Asgharpour et al. used a novel virtual card-sorting method to elicit security mental models of expert and non-experts [61]0. In this work, participants sorted 29 virtual cards with security-related words (e.g., "Spyware", "Spam") into six categories correlating to common security mental models (e.g., "Physical Safety", "Warfare"). The study revealed significant differences in mental models from these groups.

Existing elicitation methods for surfacing information reflective of real-world privacy scenarios from non-expert participants are limited [56]. To our knowledge, past research has not explored the design of engaging elements to stimulate conversations about privacy for non-experts. Brandt stresses the importance of game playing as a positive basis for learning amongst designers and users [7]. Incorporating game elements in conversations about privacy can also increase intrinsic motivation to engage in privacy topics that are otherwise often found dull [11]. Additionally, previous efforts have shown that visualizing privacy characteristics, for example through food-label style visualizations and comic strips [25][52], can be engaging and informative for users. Herein, we use low-tech tactile visual elements to elicit privacy preferences from non-expert end-users.

3 A Participatory Activities Toolkit for eliciting privacy preferences

To facilitate conversations about user privacy preferences and expectations, we developed a participatory activities toolkit that consists of three components: 1) two software prototypes that represent AATs, 2) a set of low-fidelity tangible paper-based cards and charts, and 3) instructions for using the elements described above to facilitate conversations and efficiently record user input.

The primary motivation for creating the toolkit was to develop accessible tools and protocols to help non-expert end-users reflect on and express their preferences and expectations towards the privacy characteristics of AATs. We focused on two AATs: systems that support typing and systems that support using a pointing device (e.g., a computer mouse). We chose these applications because they are common and potentially gather different types data.

In the next sections, we first describe the design process that led to the current version of the toolkit. We will then describe the different components of the toolkit including the activity procedures.

3.1 Activities Toolkit Design Process

The current toolkit is the result of an iterative design process that incorporated findings from the literature, as well as, our observations with previous research. In earlier research, we observed that discussing and communicating the privacy characteristics of adaptive applications in detail is challenging for non-technical participants [18]. To help with communication, we developed a set of icons to represent AATs' privacy characteristics. These included the types of data collected by an application. Previous research has shown the potential of using icons and graphical elements for communicating privacy characteristics of applications [25].

We next realized that we could use these icons as part of a research probe to facilitate interviews. Inspired by board and card games, in which physical elements are used to express choices and actions, we printed out the icons and created additional ones to represent third parties and privacy policies. However, we did not include gamified elements such as scores or a playful narrative. We also refrained from calling the activities "a game" to avoid trivialization of the research study [11], [37]. Finally, we combined printed cards with non-technical language and icons, as well as, charts where the cards could be arranged in an initial version of the toolkit. We conducted three pilots with participants outside of our target population to get feedback on the toolkit that helped us simplify the elements, refine the activities and work out their timing. We will describe the elements within the current version of the toolkit next.

3.2 Adaptive Assistive Technology (AAT) Prototypes

The kit consists of two software prototypes that represent AATs that participants might use to access the Internet. The prototypes are only used to describe the functionality of AATs and do not collect any user data.

We based the first AAT prototype, *SuperSpeller*, on the popular cloud-based writing assistant, *Grammarly* [16]. In addition to Grammarly's functionality of monitoring typing input and suggesting corrections, we told participants that SuperSpeller would also detect and fix errors due to typing difficulties. We used this description to elicit user feedback and did not implement the additional functionality.

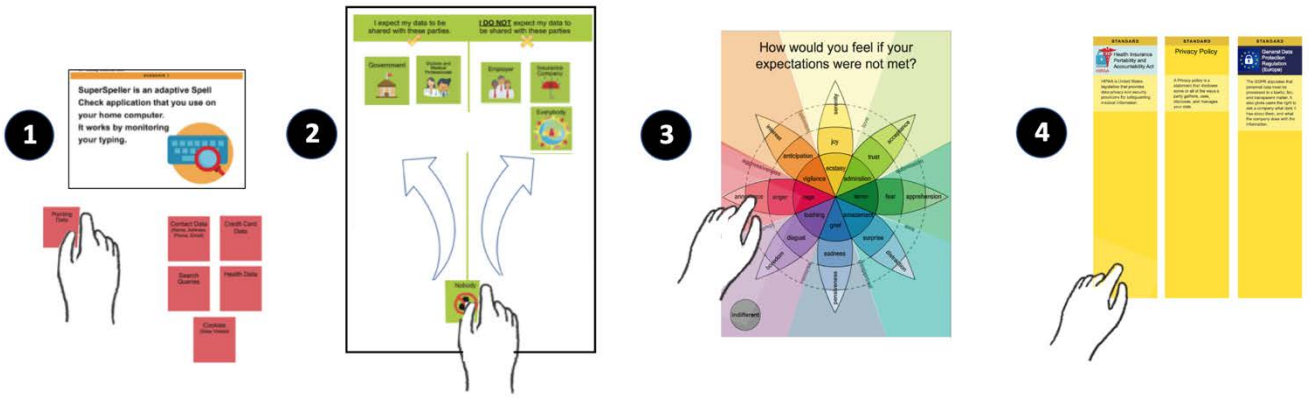

Figure 2. Overview of participatory activities. 1) First, the participant categorizes Data Type Cards according to a given Scenario Card. 2) Next, they categorize Third-Party Cards on the Expectations Chart based on who they expect to access their data. 3) Next, they use the Wheel of Emotions to describe their emotions if their expectations about third parties are not met. 4) Finally, they use the Privacy Standard Strips to describe how they want to enforce their expectations expressed on the Expectations Chars.

We designed the Pointing Interaction Notifications and AdapTAtions (PINATA) [18] to help users who experience difficulty when using pointing devices. It consists of a dynamic *bubble cursor* [17] that simulates the functionality of dynamically changing size in response to users' pointing performance and the location of the cursor. PINATA monitors a user's pointing behavior over time and when errors are detected (e.g., a link is missed while it is being clicked) increases the size of the cursor. Bubble cursors have been shown to support efficient target selection for users with and without disabilities [13]. They can provide contextual visual feedback to users (a circled area around the cursor), while not impacting the visual appearance of the underlying website, features previously found to be desirable by users of AATs for web navigation [18], [36].

3.3 Activity Cards, Privacy Standard Strips, the Expectations Chart, and the Wheel of Emotions

The second component of the kit consists of low-fidelity objects printed on paper including cards that represent data types, third parties, and scenarios, strips of paper to represent privacy standards, an Expectations Chart, and a Wheel of Emotions diagram (Figure 1). The items were printed on standard paper in full color, and used as physical objects for participants to think with [39]. Activity cards were grouped into three categories: Scenario Cards, Data Type Cards, and Third-Party Cards. To make it easy to distinguish between the categories, we printed them in different colors, each with different image to text ratios.

White *Scenario Cards* (3 x 4") summarized the functionality of each AAT application, shown in Figure 2, activity 1. Our current kit includes two scenarios cards: PINATA (i.e., an AAT to help with pointing), and SuperSpeller (i.e., an AAT to help with typing). Scenario cards have short descriptions of each AATs functionality with representative graphics.

Red Data *Type Cards* (2.5 x 2.5"), also shown in Figure 2, activity 1, represent one of seven different types of user data: Typing Data, Pointing Data, Credit Card Data, Contact Data, Health Data, Search Queries and Cookies. We included blank cards in this category, in case participants had suggestions for other data types. We purposely did not include detailed information about each data type to decrease the chance of biasing participants' perceptions.

Green *Third-Party Cards* (2.5 x 2.5"), shown in Figure 2, activity 2, contain text and graphics for ten different third-parties: Family, Friends, Doctors and Medical Professionals, Employers, Insurance Companies, Government, Private Organization that developed AAT, Advertisers, Nobody and Everybody. We included blank cards for participant suggestions for other third parties.

The *Expectations Chart* consisted of a large sheet (8.5 x 11") divided into two columns, also shown in Figure 2, activity 2. The header of the left column is titled, "I expect these parties to have access to my data," and the right column header is titled, "I do NOT expect these parties to have access to my data." This was used by participants to categorize Third-Party Cards based on their expectations for each application.

The *Wheel of Emotions* is a full-color printed (6.5 x 10") copy of Plutchik's visual framework for categorizing emotions [41], [42], shown in Figure 2, activity 3. This framework is based on the combinatory social emotion theory [51] and widely used within HCI design and research [46][27][14]. The Wheel of Emotion presents a categorical representation of 32 emotions strategically formatted onto an annular model. The middle ring holds, what Plutchik identified as, the eight primary emotions: Anger, Anticipation, Joy, Trust, Fear, Surprise, Sadness, and Disgust. Plutchik theorized that the remaining emotions are related to the primary emotions, by increasing or decreasing the intensity of those emotions [41]: emotions with increased intensity are placed in the innermost ring, while less intense emotions are placed further away. Our intention for using this element was to assess whether participants' emotional responses varies significantly across different scenarios.

Finally, the yellow *Privacy Standard Strips*, shown in Figure 2, activity 4, were the same width as Data Type Cards but longer in length (2.5 x 6"). The cards were labeled and represented seven different types of privacy standards including the Health Insurance

Portability and Accountability Act (HIPAA), the General Data Protection Regulation (GDPR), Privacy Policy, Terms of Service, Data Use Agreement, Custom Rules (for the participant to make their own standards), and No Rules. For each card, we wrote a brief non-technical description of the represented standard (please see supplement). While there is no common set of privacy standards in the literature and, in general, each domain or concern has a different set of possible standards, responses, laws or regulations, we chose the ones this study because we felt they were most likely to be relevant, but this is also why we wanted the toolkit to be open-ended enough to capture new ideas from end-user perspectives.

3.4 Participatory Activity Procedures

The kit includes a series of four activities using the components described above. The experimenter first selects a scenario card and follows the activities in sequence. Figure 2 provides a visualization of these activities. Throughout the activities, unless brought up by the participant, we did not talk about overtly positive or negative cases to avoid bias.

3.4.1 Activity 1: What Data Should an AAT Collect?

We first asked the participant what types of data they expected the AAT in the scenario card to collect. We gave them the red Data Type cards and asked them to categorize the cards based on whether they expect the application to collect them or not. We asked the participant to elaborate on why each (if any) of the data types would be collected by the application in the given scenario. Blank data type cards were offered if they wanted to include new data types.

3.4.2 Activity 2: Who Should Access my Data?

We next gave them Third-Party Cards and asked to place them on the Expectations Chart to indicate which parties should have access to their data collected by the application in the given scenario. We asked them to explain their reasoning when placing the Third-Party Cards in the chart. Blank cards were offered in case the participant wanted to add a new third party to the chart.

3.4.3 Activity 3: How Would I feel if my Expectations are not met?

Next, the participant speculated about how they would feel if their expectations, discussed in the previous activity, were not met. Participants pointed to corresponding emotions on the Wheel of Emotion if each party on a Third-Party Cards could access their data. For example, if a participant had previously placed the Advertiser Party Card in the "I do NOT expect this party to have access to my data" column, the researcher would ask them to use the Wheel of Emotions to identify how they might feel if advertisers had access to their data, and explain their response.

This activity started with the researcher demonstrating with an example and continued until the participant had located their emotions on the Wheel of Emotion for all of the available Third-Party Cards (including new ones they might have suggested in the previous activity). Once emotions for all cards were identified, the researcher would ask about groups of emotions. For example, if the participant had identified "annoyance" when third parties would access their data, the researcher might ask if they can identify provisions with their data is that would make them feel less annoyed.

3.4.4 Activity 4: What Standard(s) should Protect my Data?

In the last activity, participants selected privacy standards to protect their data. The researcher would begin the activity by placing all yellow Privacy Standard Strips in front of the participant and read a brief description of each standard. Participants were asked to identify and explain which standards they would like to be enforced. Next, the researcher would bring back the completed Expectations Chart from the previous activity and ask the participant how they would like their selected standards to guide third party handling of their data. Finally, the participant used the Wheel of Emotions to describe how they would feel if their chosen standards were implemented by the application.

4 Participatory Activities Toolkit Evaluation

We used the participatory activities toolkit to understand the perspectives of individuals who experience difficulties accessing the Internet. We first present participant information, followed by descriptions of our data collection and analysis activities.

4.1 Participants

We recruited six adult participants, age 65 years or older, who experience diverse pointing and typing difficulties (Table 1). Initially, we recruited eight participants but two of them opted out before the completion of the study. The participants were recruited from a local organization in a large metropolitan city in the United States that provides support to individuals with Essential Tremors (ET) and had participated in a previous study we had conducted [18]. The participants had not been asked about different adaptive applications and had not seen the participatory activities toolkit prior to this study. None of the participants had used AATs beyond our research study. The participant selection requirement of older adults with ET who could meet in person with us limited the number of participants but allowed us to focus on the privacy perspectives of individuals with a sensitive health diagnosis.

Essential Tremors (ET) is a chronic, progressive neurological disease, manifesting as a kinetic tremor [33][32]. Nearly seven million individuals in the United States (approximately 2% of the population) are estimated to have Essential Tremors, and it is the most widespread form of movement disorder in the world [32], yet this group is underrepresented in accessibility and privacy research. The effects of ET are typically experienced gradually and can impact employment and access to computers adversely. People with ET are known to choose premature retirement and forgo application for a promotion or new job opportunity because of uncontrollable shaking from tremors [4], [43]. Because of these conditions, individuals experiencing ET may be motivated to adopt assistive technologies that help them compensate for their changing abilities, and yet be reluctant to disclose their health information to

Table 1. This table provides information about the 6 participants with essential tremors who took part in the study.

Participant ID	*Age*	*Gender*	*Career History*	*Reason for Pointing Difficulty*	*Weekly Internet Use (hours)*	*Perceived Value of Internet Access*
P1	71	Female	Customer Service	Essential Tremors	2 Hours	Somewhat Valuable
P2	82	Male	Forestry	Essential Tremors	25-30	Somewhat Valuable
P3	69	Male	Geology, Computer Tech, Army, Peace Corps	Essential Tremors	30+ Hours	Very Valuable
P4	87	Male	Air Force Pilot, Computer Specialist, Accountant	Essential Tremors	8-9 Hours	Very Valuable
P5	64	Female	Computer Systems Analyst, Stay-at-Home Mom, Fitness Tech	Essential Tremors	12-14 Hours	Very Valuable
P6	73	Male	Educator (University)	Essential Tremors	14-28 Hours	Very Valuable

employers or insurance companies. We also considered them to be a population that would be aware of privacy issues regarding disclosing their diagnosis or ability.

Every participant reported experiencing intermittent difficulty when using a pointing device and/or a keyboard. None of the participants reported impairments that completely impeded computer use. All participants considered themselves to be retired at the time of the study (except P1 who was employed part-time). All participants had experience using computers both in their careers and during retirement.

4.2 Interview Procedures

We conducted six semi-structured in-person interviews lasting 58 minutes on average and ranging from 31 to 76 minutes. We interviewed participants about the history, nature, and frequency of their difficulties when using computers, including past and present computer use, career history, and if and how computer use difficulties impacted their career or personal use. We used the four activities described in Section 3 for SuperSpeller (Scenario 1) and PINATA (Scenario 2).

4.3 Data Collection and Analysis

We audio recorded and transcribed each session, with the exception of P4 (we instead took detailed notes at their request) and photographed participants' completed Expectation Charts and Wheel of Emotion. The photographs and transcriptions were used to depict the data into ten visualization boards for each participant, totaling 60 visualization boards. We used the boards to visually represent participants' preferences in the Expectations Chart (e.g., Figure 3), their expressed emotions using the Wheel of Emotions, and their selected privacy standards. We used the boards to efficiently corollate the data with interview results.

We conducted an iterative thematic analysis to identify and synthesize themes within the interview transcriptions [6]. The researcher who conducted the interviews transcribed them and conducted the first round of coding. This process included noting keywords, prominent emerging themes, supporting anecdotes, and patterns. Other members of the research team conducted a second round of coding where we further analyzed the existing themes and identified new ones. Once the second coding phase was complete, we organized the findings across five themes and seven subthemes presented next.

Figure 3. A sample Expectation Chart visualization board (P4)

5 Findings

5.1 Activity 1: What Data Should be Collected by AATs?

Participants expected each AAT to only collect data related to the activity it is meant to support: They expected SuperSpeller to collect typing data and PINATA to collect pointing data. The following findings illustrate how the premise under which an application is presented to and chosen by users impacts their expectations towards what types of data it would collect.

Most participants expected SuperSpeller to collect data in addition to typing statistics or keystrokes, including contact data (P1, P3, P4, and P6), search queries (P1, P3, P4, P5), cookies (P1, P3, P5) and credit card information (P5). In contrast, participants expected much less data to be collected by PINATA. Only two participants (P1, P6) expected that PINATA would collect typing data in addition to pointing data. P5 illustrates this contrast: She expected SuperSpeller to collect all types of data represented by the Data Cards. However, she expected PINATA to only collect pointing

data, describing that other types of data are not directly related to its functionality.

Participants expressed different perceptions of how the applications would use the collected data. For SuperSpeller, all participants thought it would collect spelling and grammar errors. They also described more detailed ways that the application would detect performance, including collecting the content of what is typed (P1, P2, P5), tracking keys that are held down too long (P6), noting repeated typing errors of the same nature (P6), and learning a user's speech pattern (P1). For PINATA, participants expressed that the application might monitor their general pointing performance (P1, P3, P5, P6), detect the severity of their shaking (P1, P3), determine errors patterns based on the time of day (P1), target clicking patterns (P2, P4), and the degree of overshooting or undershooting an onscreen target (P3).

Only one participant (P5) initially identified the possibility of the AATs collecting data that could be related to a health condition. However, after participating in the activities all participants wavered on their initial opinion. Throughout the activities, participants experienced shifting perspectives about how much AATs could or should know about their health condition. For example, while P4 initially stated that the AATs cannot know about her ET diagnosis through monitoring her performance data, she later expressed this as a possibility that could inform her doctors and medical professionals better about her condition:

> "If my [ET] got worse and [doctors] needed to prove that I have this condition-- if they had access to PINATA, it might be able to show them." -P4

Others described how the AATs could detect their health conditions. For example, P2 described how SuperSpeller could link his typing data to his health condition:

> "Say you're on the internet and you're googling some health thing-- Somebody could say, 'Oh, they're asking that (question about health condition)!? He's got that, that, and that! (specific health conditions)"

Some participants expressed concern once they realized their performance data could be linked to a specific health condition. For example, once P1 realized PINATA could detect his degree of shaking and relate it to ET, he stated:

> "I don't see where any of this [health data] pertains to anything they're doing with [PINATA]."-P1

Others (P2, P3, P6) were quite clear that neither of the AATs should collect health data or link collected data to a specific health condition.

> "[AATs] should not have access to [your] medical information, unless you want them to." -P2

All participants described how some of their performance data (e.g., typing errors, pointing patterns, etc.) could be linked to specific neurological conditions.

5.2 Activity 2: Who Should Have Access to My Data?

Participants expressed diverse preferences about who they were comfortable having access to data collected by each AAT (Table 2). Overall, they were more receptive to their data being shared with the developers of the assistive technology and with medical professionals, and most did not want their data to be accessed by other third parties. Additionally, participants were more open to sharing data collected by PINATA than by SuperSpeller. We next present participants' sharing preferences by scenario.

Table 2. Summary of data sharing preferences for PINATA (PI) or SuperSpeller (SS). Participants were most comfortable sharing data with assistive tech companies and medical professionals.

	Yes		Maybe		No	
Application	**PI**	**SS**	**PI**	**SS**	**PI**	**SS**
Private Assistive Tech Company	3	2	2	1	1	3
Medical Professionals	3	0	1	2	2	4
Employers	0	0	1	1	5	5
Government	1	0	0	1	5	5
Insurance Companies	0	1	0	0	6	5
Advertisers	1	1	0	0	5	5
Family Members	1	0	0	0	5	6
Friends	0	0	0	0	6	6

5.2.1 Sharing Typing Data

Participants were more protective of their typing data than pointing data and viewed it to be more personal. P2, P4, P5 did not want anyone to have access to their typing data. P2 and P5 stated that they could not justify why an AAT would need so much information, while P4 she identifies as a "*private person*" who did not "*want just anybody going and looking at [my data]*."

In contrast, the rest of the participants (P1, P3, P6) were comfortable with the assistive technology company that developed the AAT to collect and use this data to improve system usability. P6 specified that she would be comfortable with the company using her data with her consent and only used it to improve system usability. Similarly, while P1 was willing to share his typing data, he had a strong preference for strict data privacy standards:

> "I think they're doing something useful… I think they need the data to do the program. But then, I wouldn't want them to share [my data] with these [pointing to other Third-Party cards]." - P1

Beyond the application's developer, participants did not want other third parties to access their data. Only one participant (P6) stated that she might be comfortable with her employer having access to her typing data if they asked for her consent. Other participants described a lack of trust and fear of negative employment repercussions as reasons to not share with an employer.

Most Participants (5) did not want their typing data shared with insurance companies because they believed it would be used to "*enhance their bottom line*" (P1), or be interpreted as incorrect evidence for the existence of a health condition:

> "I don't want [insurance companies] predicting that I have Parkinson's Disease, or something, and they don't know what the diagnosis is-- nor do they need to." -P6

Most participants (5) expressed fatigue and annoyance from digital advertising and did not want advertisers to access their typing data.

Most participants (5) expressed that they did not want the government to access their typing data, sometimes referring to specific departmental agencies, for example the National Security Agency (NSA) or the Internal Revenue Service (IRS). One participant (P3) stated he would be comfortable with the government having access to his typing data if they had "*some kind of subpoena, warrant, or probable cause*."

No participant expected their friends or families to have access to their typing data collected by the application, citing personal privacy, and seeing no reason why such access would be useful:

> "Friends: don't need [my typing data]. Family: I might want to be the one to present it to them (rather than the AAT)." -P6

5.2.2 Sharing Pointing Data

Participants were initially generous in sharing their pointing data, although these preferences shifted once a participant realized this data could be linked to a health condition. All but one participant (P4) were comfortable sharing their data with the private company either under no conditions or with explicit permission. All participants thought their data could be used to improve and update the AATs performance.

> "I'd be okay with [private company] using my data to fine-tune [the AAT]. How else are they going to get the feedback?" -P6

Half of the participants (P1, P3, P4) were also comfortable sharing their pointing data with their doctors and medical professionals, as a valuable source of information about their health condition:

> "They're the ones that are going to help, and if they don't have access, how are they going to do that?" - P1

> "[I'd share my data] if it meant getting a better understanding of whatever condition you have." -P4

Only one participant (P3) was comfortable with the government having access to their pointing data. P3 believed certain agencies within the government could aggregate this data to benefit him (and others with similar difficulties).

All participants (5) did not want advertisers to have access to their pointing data because they did not believe it would have any benefits for them. P1 stated that he could not see harm in sharing his data with advertisers:

> "I just don't know what an advertiser would need or want it for, but I don't think they would do any harm with it." -P1

All participants, (5) did not want employers to have access to their pointing data, describing scenarios in which this could result in harmful consequences at work.

> "I think it would affect your job possibilities… [I know someone who] was fired from a job because he's got a voice tremor." -P1

P6 expressed a different perspective, that consensual access to her pointing data could assist in identifying what accommodations she may need in the workplace.

No participants were comfortable with insurance companies accessing their data, stating unjustified data extrapolations (P1), increased rates (P1), insurance bias (P3), and unreliably concluding they have a health condition (P6) as potential harmful consequents:

> "Here's what I fear: If you can't point your finger with the computer, are you going to be able to steer, okay? Should we make your insurance more expensive because you're going to have an accident? -P1

> "I want them to get [my performance data] from a neurologist, not from a generalized tool." -P6

Finally, participants did not want their friends and family to access their data, describing that as a violation of privacy.

5.3 Activity 3: How Would I feel if my Expectations are not met?

Participants used the Wheel of Emotion to express a range of emotions if their expectations were not met in each scenario. The most common emotional reactions when discussing SuperSpeller sharing their pointing data, was annoyance (5), anger (P3, P5, P6), disgust (P2, P4), surprise (P3, P6), acceptance (P1, P6). Participants exhibited the most intense emotional responses towards the government accessing their personal typing data without their consent, offering that they would feel anger (P3, P5), fear and terror (P1), disgust (P2), violation (P4), and annoyance (P3, P5, P6).

Participants expressed less intense, albeit still negative, emotions about their pointing data being shared. Most participants again expressed annoyance (5), apprehension (P2, P3) acceptance (P2, P6), anger (P4), sadness (P4), violation (P4), surprise (P6) indifference (P1), and fear (P1). Participants expressed fear (P1), apprehension (P2), and annoyance (P3, P4, P5, P6) if their typing data were accessed by insurance companies. They expressed fear and terror (P1), apprehension (P2, P3), violation (P4), annoyance (P4, P5), and acceptance (P6), if employers were allowed to access their pointing data.

5.4 Activity 4: What Standard(s) should Protect my Data?

All participants selected two or more privacy standards (median of three) to guide how their data is collected in both scenarios. We present their preferences below.

5.4.1 Health Information Portability and Accountability Act (HIPAA)

Our team was surprised that only two participants (P4 and P6) wanted AATs to abide by the HIPAA standard. P1 and P3 described negative past experiences with HIPAA and considered it cumbersome. P3 described how using HIPAA can make communication and data sharing between health professionals difficult. P2 and P5 viewed it as irrelevant for the AATs under study. For example, P2 stated the HIPAA should be used if "*you want to do something with your health insurance*." P4 and P6 were enthusiastic about AATs abiding by HIPAA. For example, P6 described how HIPAA can be useful since it is "*producing some good restraints on how the data [is accessed] already.*"

5.4.2 General Data Protection Regulation (GDPR)

Four participants (all but P1 and P2) wanted both AATs to abide by GDPR and had several reasons for choosing it. P3 believed it provided more agency, saying "[with GDPR] *the focus is … on the user's right to inquire or raise issues … so I would like that.*" P5 believed GDPR was "*simple and sensible*", and that "*if you're wondering what's going on, you can ask them.*" Finally, P6 believed GDPR requires companies to be transparent about what data it is collecting and what it had collected. Participants who did not select GDPR stated that they were too unfamiliar with it (even after our description).

5.4.3 Other Privacy Standards

In addition to HIPAA and GDPR, participants considered a Privacy Policy, Terms of Service, Data Use Agreement, Custom Rules, and No Rules. All participants stated some form of privacy standard that the AATs should abide by. Three participants (P1, P2, P5) selected one of the agreement/disclosure standards, while the rest chose a combination of these standards (P3, P4, P6). Two of the participants (P1, P2) did not choose existing standards such as GDPR or HIPAA. Participants described wanted standards that protected their data against unauthorized access, gave control over their data, and provided transparency on how data is used. For example, P2 selected a Privacy Policy with the added requirement that it ensure that his data would remain anonymous and inaccessible to any third parties, which represents more stringent protection than under either HIPAA or GDPR. P5 chose a Terms of Service Agreement over a Privacy Policy because it provided her with more control and agency:

> "Privacy policy is telling me what it's going to do, but [terms of service] is asking me to agree to it, so I like that better. The company agrees that the program will not send [my] data to anyone without asking me first." -P5

Some participants sought to combine standards to control their data. For example, P3 described a Data Use Agreement nested within a Privacy Policy, providing specific choices on who should access his data:

> "I'd really want to know the purpose and intent of friends, insurance companies, and employers' interest in having that data available, and be able to evaluate that in each individual case, rather than grant blanket permission."

In summary, participants saw the role of privacy standards as enforcing user agency and decision making and increasing application developers' transparency.

5.5 Participatory Activities Toolkit Reflection

Participants received the participatory activities toolkit positively, and we found it effective at eliciting detailed preferences and expectations. The activities were easy to deploy, and the participants used some of the kit's components creatively to add their own content to it. We also noted several opportunities for future improvements.

5.5.1 Attitudes towards Tactile Visual Components

Four participants (P3, P4, P5, P6) found the activities helped reflect on their preferences and express them in detail. Several described the kit as "*thought-provoking*" (P3, P6), "*eye-opening*" (P4) and helpful to clarifying expectations:

> "[The activity kit] does actually make you try to think about the stuff and try to clarify your own thinking." -P5

Participants gave positive feedback on the tactile aspect of moving physical printed cards around the Expectation Board and Wheel of Emotion. Preferring tactile activities to an interview, P6 said:

> "[The activities] kept my attention better than just reading or answering questions without having something to move around...I liked having something to pick up and move." -P6

P4 used the toolkit to express his emotions in playful ways. He picked up the Government Third-Party Card, announced, "*and these people*…," assertively smacking the card down into the "I do NOT expect them to access my data" column of the Expectation Chart, and chuckled.

Participants used the blank cards we provided to add new elements to the kit. Two participants (P4, P5) created new activity cards. P5 made an additional Third-Party card representing technology companies other than the one that developed the AAT who shouldn't access his data.

> "Generalized tech companies like Google or Facebook… They have their own ends for [my data], I suppose. ... It's none of their business. They'd think of something unpleasant to do with [my data], no doubt." -P5

P4 made an additional Data Type Card representing her banking data, discussing the importance of keeping this data private. She did not want her banking data, or any data that could be used to access her banking data, collected by AATs.

We observed some creative uses of the toolkit. For example, two participants (P3, P6) placed Third-Party Cards on the division line in the center of the Expectations Chart. They said their decision about whether these parties could access their data depends on the conditions and agreements put on their access. This highlights the flexibility of the toolkit to represent complex privacy expectations, which is crucial because privacy is subjective.

5.5.2 Expressing Emotions using the Toolkit

Most participants (4) effectively used the Wheel of Emotion to express a range of emotions (as described above). However, two participants (P3, P5) found the Wheel of Emotion hard to use.

> "I'm surprised that certain words are put in certain places. It wasn't always easy to find what I thought was most appropriate." -P3

P5 found it difficult to project how he would feel without having actually experienced a proposed scenario in real life, and P3 found it difficult to navigate the wheel.

6 Discussion

6.1 Eliciting End-User Privacy Perspectives

The participatory activities toolkit was effective at eliciting detailed responses about privacy preferences and expectations and helping end-users reflect on privacy tradeoffs. Participants had positive attitudes towards the activities with several describing them as thought-provoking and engaging and commenting that they made it easier to think and talk about privacy. Several participants used the cards in new ways, by moving them forcefully to emphasize a point or by placing them in ambiguous parts of the Expectations Chart. They also moved the physical cards when shifts happened in their preferences. Finally, participants used the provided blank cards to suggest new third-parties and data types. We believe seeing the cards in relation to each other supported reflection.

Participants identified difficulties with the toolkit and made suggestions for improvement. Specifically, they found the Wheel of Emotion difficult to use and wanted simpler tools to express emotion. Other research (published after our study) found the Circumplex Model of Emotion, easier to use for design activities than the Wheel of Emotion [21]. The Circumplex Model is a scheme that situates emotions along the two dimensions of arousal and valence [47]. While we plan to experiment with the Circumplex Model and a simplified Wheel of Emotion in the future, the toolkit may also be used without this component (i.e., without Activity 3).

6.2 AATs' Dangerously Ambiguous Double-Role as Productivity and Accessibility Tool

Our findings highlight a troubling lack of end-user clarity on the premise under which personal data is collected and how this ambiguity can lead to privacy threats. While most participants were initially receptive to the idea of using their data to improve system functionality for themselves and others with similar health conditions, they were unpleasantly surprised by the prospect of their data being shared with third parties and used for other purposes. They described negative scenarios where this could lead to inaccurate medical diagnosis or unwanted disclosure with serious consequences such as losing a job or being disqualified by insurance. Furthermore, most participants expressed intense negative feelings, such as anger and disgust, about these scenarios.

These findings are in-line with past research that reported users' feelings of creepiness and panic upon learning their data was used for purposes other than the premise under which it was originally collected [2], [50]. Our work contextualizes privacy threats for accessibility apps and underlines the danger of exposing an underserved and vulnerable population to serious privacy threats. Disability activists have been vocal about the potential abuse of emerging technologies as tools of discrimination and marginalization [49][63]. Our findings highlight the urgent need to recognize and address the dangers of collecting usability and performance data from people with disabilities.

6.3 Privacy Implications of Personal Data

Participants expected each AAT to collect and use data types relevant to its functionality: they expected the SuperSpeller to collect typing data and PINATA to collect pointing data. This expectation informed their privacy concerns about each AAT; while most participants were wary of SuperSpeller sharing collected data, they assumed might include sensitive information such as credit card information and search queries, they were initially less concerned PINATA sharing their pointing data or even collecting other types data. Once participants reflected on these possibilities, they became more concerned about the way AATs collect and share data and expressed the need and desire for ways to control, monitor and authorize them.

These shifts in participant perspectives illustrate a need to provide end-users with control and agency over their personal data. Users must be informed about what data is being collected and the risks of collecting this data. This could be managed by including customizable data collecting/sharing features that empower users to specify how their data is managed.

6 Limitations and Future Work

We plan to adapt and use the toolkit with other populations, including younger adults with disabilities. We can then compare their perspectives with the current results and also explore how to customize the toolkit. Given that user opinions frequently change due to self-education and societal trends, we are also planning a longitudinal study. Finally, we plan to share the toolkit with other researchers, using online printable templates, prototype software repositories, and video instructions on how to use it.

7 Conclusion

There is a growing interest in capitalizing on usability gains of adaptive assistive technologies (AATs) by collecting, aggregating and incorporating user data. These gains need to be positioned in relation to privacy threats that collecting such data can expose users to. To better understand these threats from end-user perspectives, we developed and utilized a participatory activities toolkit that uses tactile visual elements to facilitate conversations about privacy. We conducted a study with 6 older participants who have difficulty using typing and pointing devices. The results showed that the toolkit was effective at facilitating conversations and reflections on privacy, further underlining the importance of participatory and inclusive approaches towards the privacy of emerging technologies.

REFERENCES

[1] (Farzaneh Asgharpour, Debin Liu, and L. Jean Camp. 2007. Mental Models of Security Risks. In *Proceedings of the 11th International Conference on Financial cryptography and 1st International conference on Usable Security* (FC'07/USEC'07), 367-377.

[2] (Julio Angulo and Martin Ortlieb. 2015. "WTH..!?!" Experiences, Reactions, and Expectations Related to Online Privacy Panic Situations. In *Proceedings of the 11th Symposium on Usable Privacy and Security* (SOUPS '15), 19-38.

[3] (Shiri Azenkot, Kyle Rector, Richard Ladner, and Jacob Wobbrock. 2012. Pass-Chords: Secure Multi-touch Authentication for Blind People. In *Proceedings of the 14th International ACM SIGACCESS Conference on Computers and Accessibility* (ASSETS '12), 159–166.

[4] (P. G. Bain, L. J. Findley, P. D. Thompson, M. A. Gresty, J. C. Rothwell, A. E. Harding, C. D. Marsden. 1994. A study of hereditary essential tremor. *Brain* 117(Pt 4), 805–824.

[5] (Ur Blasé, Pedro G. Leon, Lorrie F. Cranor, Richard Shay, and Yang Wang. 2012. Smart, useful, scary, creepy: Perceptions of online behavioral advertising. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (SOUPS '12), Article 4.

[6] (Richard E. Boyatzis. 1998. *Transforming Qualitative Information: Thematic Analysis and Code Development.* Sage Publications, Inc.

[7] (Eva Brandt. 2006. Designing Exploratory Design Games: A Framework for Participation in Participatory Design? In *Proceedings of the Ninth Participatory Design Conference*, 57-66.

[8] (Fred H. Cate. 2006. The Failure of Fair Information Practice Principles. *Social Science Research Network*, Rochester, NY, SSRN Scholarly Paper ID 1156972.

[9] (Lorrie F. Cranor. 2005. Giving Notice: Why Privacy Policies and Security Breach Notifications Aren't Enough. *IEEE Communications Magazine*, 43 (8), 18–19.

[10] (Yngve Dahl and Kristine Holbø. 2012. "There are no secrets here!": Professional stakeholders' views on the use of GPS for tracking dementia patients. In *Proceedings of the 14th International Conference on Human-Computer Interaction with Mobile Devices and Services* (MobileHCI'12), 133–142.

[11] (Filomena Faiella and Maria Ricciardi. 2015. Gamification and learning: a review of issues and research. *Journal of e-Learning and Knowledge Society*. 11 (3), Italian e-Learning Association.

[12] (Federal Trade Commission. 2000. *Privacy Online: Fair Information Practices in the Electronic Marketplace.*

[13] (Leah Findlater, Alex Jansen, Kristen Shinohara, Morgan Dixon, Peter Kamb, Joshua Rakita, and Jacob O. Wobbrock. O. 2010. Enhanced area cursors: reducing fine pointing demands for people with motor impairments. In *Proceedings of the 23nd annual ACM symposium on User interface software and technology* (UIST '10), 153-162.

[14] (Valentina Franzoni, Alfredo Milani, and Giulio Biondi. 2017. SEMO: A Semantic Model for Emotion Recognition in Web Objects. In *Proceedings of the International Conference on Web Intelligence* (WI '17), 953-958.

[15] (Nanna Gorm and Irina Shklovski. 2016. Sharing Steps in the Workplace: Changing Privacy Concerns Over Time. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (CHI '16), 4315-4319.

[16] (*Grammerly*. Retrieved February 21, 2019 from https://www.grammarly.com/

[17] (Tovi Grossman and Ravin Balakrishnan. 2005. The Bubble Cursor: Enhancing Target Acquisition by Dynamic Resizing of the Cursor's Activation Area. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '05), 281-290.

[18] (Foad Hamidi, Kellie Poneres, Aaron Massey, and Amy Hurst. 2018. Who Should Have Access to my Pointing Data?: Privacy Tradeoffs of Adaptive Assistive Technologies. In *Proceedings of the 20th International ACM SIGACCESS Conference on Computers and Accessibility* (ASSETS '18). ACM, New York, NY, USA, 203-216.

[19] (Jim Harper. 2004. Understanding Privacy – And the Real Threats to It. *Cato Policy Analysis* 520, p. 20.

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

[21] (Jennifer Healey, Pete Denman, Haroon Syed, Lama Nachman, and Susanna Raj. 2018. Circles vs. Scales: An Empirical Evaluation of Emotional Assessment GUIs for Mobile Phones. In *Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services* (MobileHCI '18), Article 12, 11 pages.

[22] (Scott Hollier and Shadi Abou-Zahra. Internet of Things (IoT) as Assistive Technology: Potential Applications in Tertiary Education. In *Proceedings of the 15th International Cross-Disciplinary Conference on Web Accessibility* (W4A '18). ACM, New York, NY, USA, 4 pages.

[23] (Carlos Jensen and Colin Potts, 2004. Privacy Policies as Decision-making Tools: An Evaluation of Online Privacy Notices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, New York, NY, USA, 471–478.

[24] (Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. In *Proceedings of the 11th Symposium On Usable Privacy and Security* (SOUPS '15), 39-52.

[25] (Patrick G. Kelley, Lucian Cesca, Joanna Bresee, and Lorrie F. Cranor. 2010. Standardizing privacy notices: An online study of the nutrition label approach. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '10), ACM, New York, NY, USA, 1573–1582.

[26] (Alfred Kobsa. 2007. Privacy-enhanced personalization. *Commun. ACM*, 50 (8), 24-33.

[27] (Fajri Koto and Mirna Adriani. 2015. HBE: Hashtag-Based Emotion Lexicons for Twitter Sentiment Analysis. In *Proceedings of the 7th Forum for Information Retrieval Evaluation*, 31-34.

[28] (Ruth Landau, Gail K. Auslander, Shirli Werner, Noam Shoval, and Jeremia Heinik. 2010. Families' and professional caregivers' views of using advanced technology to track people with dementia. *Qual. Health Res*. 20, 3 (March 2010), 409–419.

[29] (Ruth Landau, Shirli Werner, Gail K. Auslandei Noam Shoval, and Jeremia Heinik. 2009. Attitudes of family and professional care-givers towards the use of GPS for tracking patients with dementia: An Exploratory study. *Br. J. Soc.* 39, 4 (June 2009), 670–692.

[30] (Hosub Lee and Alfred Kobsa. 2017 Privacy preference modeling and prediction in a simulated campuswide IoT environment. In *IEEE International Conference on Pervasive Computing and Communications* (PerCom' 17), 276–285.

[31] (Lesa Lorenzen-Huber, Mary Boutain, L. Jean Camp, Kalpana Shankar, and Kay H. Connelly. 2011. Privacy, technology, and aging: a proposed framework. *Ageing International* 36 (2), 232-252.

[32] (Elan D. Louis, L. Barnes, S. M. Albert, L. Cote, F. R. Schneier, S. L. Pullman, and Q. Yu. 2001. Correlates of functional disability in essential tremor. *Mov. Disord.* 16, 914–920.

[33] (Elan D. Louis and Ruth Ottman. 2014. How many people in the USA have essential tremor? Deriving a population estimate based on epidemiological data. *Tremor Other Hyperkinet Mov* (4), 259.

[34] (Andrew McNeill, Pam Briggs, Jake Pywell, and Lynne Coventry. 2017. Functional Privacy Concerns of Older Adults about Pervasive Health-Monitoring Systems. In *Proceedings of the 10th International Conference on PErvasive Technologies Related to Assistive Environments* (PETRA '17), 96-102.

[35] (Aleecia M. McDonald and Lorrie F. Cranor, 2008. The Cost of Reading Privacy Policies. *I/S: A Journal of Law and Policy for the Information Society*, vol. 2008 Privacy Year in Review Issue.

[36] (Aqueasha Martin-Hammond, Abdullah Ali, Catherine Hornback, and Amy Hurst. 2015. Understanding design considerations for adaptive user interfaces for accessible pointing with older and younger adults. In *Proceedings of the 12th Web for All Conference* (W4A '15), Article 19, 10 pages.

[37] (Todd D. Nelson. 2005. Ageism: Prejudice Against Our Feared Future Self. *Journal of Social Issues*, 61 (2), 207-221.

[38] (Richard Pak, and Anne C. McLaughlin. 2010. *Designing displays for older adults.* Boca Raton, FL: CRC Press.

[39] (Seymour Papert. 1980. *Mindstorms – Children, Computers and Powerful Ideas.* New York, Basic Books Inc. Publishers.

[40] (Pew Research Center. 2017. *Automation in Everyday Life.*

[41] (Robert Plutchik. 1994. *The Psychology and Biology of Emotion*. HarperCollins College Publishers.

[42] (Robert Plutchik. 2001. The Nature of Emotions: Human emotions have deep evolutionary roots, a fact that may explain their complexity and provide tools for clinical practice. *American Scientist* 89 (4), 344-350.

[43] (Ilkka Rautakorpi. 1978. Essential Tremor. An Epidemiological, Clinical and Genetic Study. Finland: Academic Dissertation University of Turku.

[44] (Hirak Ray, Flynn Wolf, Ravi Kuber and Adam J. Aviv. 2019. "Woe is me:" Examining Older Adults' Perceptions of Privacy. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts* (CHI'19 Extended Abstracts), May 2019

[45] (Ling Rothrock, Richard Koubek, Frederic Fuchs, Michael Haas, and Gavriel Salvendy. 2010. Review and reappraisal of adaptive interfaces: Toward biologically inspired paradigms. *Theoretical Issues in Ergonomics Science*, 3(1), 47-84.

[46] (Nina Runge, Dirk Wenig, Marius Hellmeier, and Rainer Malaka. 2016. Tag Your Emotions: A Novel Mobile User Interface for Annotating Images with Emotions. In *Proceedings of the 18th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct* (MobileHCI '16), 846-853.

[47] (James A. Russell. 1980. A Circumplex Model of Affect. *Journal of personality and social psychology*, 39 (6), 1161.

[48] (Sam Schechner and Mark Secada. 2019. You Give Apps Sensitive Personal Information – Then They Tell Facebook. *The Wall Street Journal*. https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636 Accessed: April 15, 2019.

[49] (Hampus Sethfors. 2019. Apple's new Feature is a Step Towards Digital Apartheid. From: https://axesslab.com/digital-apartheid/ Accessed: April 4, 2019.

[50] (Irina Shklovski, Scott D. Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. 2014. Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '14), 2347-2356.

[51] (Andreas Schneider, Herman Smith. 2009. Critiquing Models of Emotions. *Sociological Methods & Research,* 37 (4), 560-589.

[52] (Madiha Tabassum, Abdulmajeed Alqhatani, Marran Aldossari, and Heather Richter Lipford. 2018. Increasing User Attention with a Comic-based Policy. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (CHI '18). ACM, New York, NY, USA, Paper 200, 6 pages.

[53] (U.S. Health Insurance Portability and Accountability Act (HIPAA). 1996. Pub. L. No. 104–191, 110 Stat. 1936 (1996).

[54] (Lin Wan, Claudia Müller, Dave Randall, and Volker Wulf. 2016. Design of A GPS Monitoring System for Dementia Care and its Challenges in Academia-Industry Project. *ACM Trans. Comput.-Hum. Interact*. 23, 5, Article 31 (October 2016), 36 pages.

[55] (Yang Wang. Retrieved February 21, 2019 from http://inclusiveprivacy.org

[56] (Yang Wang. 2017. The Third Wave?: Inclusive Privacy and Security. In *Proceedings of the 2017 New Security Paradigms Workshop*, 122-130.

[57] (Yang Wang. 2018. Inclusive Security and Privacy. *IEEE Security & Privacy*, 16 (4), 82-87.

[58] (Rick Wash and Emilee Rader. 2015. Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security* (SOUPS'15), 309-325.

[59] (Rick Wash. 2010. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (SOUPS '10), Article 11, 16 pages.

[60] (Ryan W. White, P. Murali Doraiswamy, and Eric Horvitz. 2018. Detecting neurodegenerative disorders from web search signals. *npj Digital Medicine* 1(1), 8.

[61] (Richmond Y. Wong, Deirdre K. Mulligan, Ellen Van Wyk, James Pierce, and John Chuang. 2017. Eliciting values reflections by engaging privacy futures using design workbooks. In *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW, Article 111.

[62] (Workshop on Inclusive Privacy and Security. 2018. http://inclusiveprivacy.org/wips2018.html

[63] (Marco Zehe. 2014. Why Screen Reader Detection on the Web is a Bad Thing. From: https://www.marcozehe.de/2014/02/27/why-screen-reader-detection-on-the-web-is-a-bad-thing/ Accessed: April 4, 2019.

[64] (Wei Zhou and Selwyn Piramuthu. 2014. Security/Privacy of Wearable Fitness Tracking IoT Devices. In *Proceedings of the 9th Iberian Conference on Information Systems and Technologies* (CISTI '14), 1-5.