EXPLORING OLDER ADULTS' ATTITUDES TOWARDS PRIVACY OF ADAPTIVE ASSISTIVE TECHNOLOGIES

By

Kellie Nicole Gable Poneres

Thesis submitted to the Faculty of the Graduate School of the University of Maryland, Baltimore County, in partial fulfillment of the requirements for the degree of

Human-Centered Computing

2018

(Sample of Approval Sheet)

APPROVAL SHEET

Title of Thesis: Exploring Older Adults' Attitudes Towards Privacy of Adaptive Assistive Technologies

Name of Candidate: Kellie Gable Poneres
Master of Science, 2018

Thesis and Abstract Approved: (*Signature of Supervising Professor)
Dr. Aaron Massey
(Rank of Supervisor)
(Name of Department or Program)

Date Approved: _____

Curriculum Vitae

Name: Kellie Nicole Gable Poneres

Degree and date to be conferred: M.S., 2018

Secondary education:
Chesapeake Senior High School, Pasadena, Maryland, 2008

Collegiate institutions attended:
Stevenson University, Bachelor of Science, 2012
University of Maryland, Baltimore County, Master of Science, 2018

Major: Human-Centered Computing.

Professional Publications:

- **The User Privacy of Adaptive Assistive Technologies.**
  Foad Hamidi, Kellie Poneres, Aaron Massey, Amy Hurst.
  In *Proceedings of the 3rd Workshop on Usable Privacy and Security (SOUPS'18).*
  Baltimore, MD. August 12-14, 2018.
  (Acceptance rate: N/A.)

- **Who Should Have Access to my Pointing Data? Privacy Tradeoffs of Adaptive Assistive Technologies.**
  Foad Hamidi, Kellie Poneres, Aaron Massey, Amy Hurst.
  In *Proceedings of the 20th International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS'18).*
  Galway, Ireland. October 22-24, 2018.
  (Acceptance rate: 25%.)

- **Using Icons to Communicate Privacy Characteristics of Adaptive Assistive Technologies.**
  Kellie Poneres, Foad Hamidi, Aaron Massey, Amy Hurst.
  In *Proceedings of the 20th International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS'18).*
  Galway, Ireland. October 22-24, 2018.
  (Acceptance rate: 50%.)

Professional positions held:

- October 2014 - Present.
  Web and Graphic Designer for Public Awareness Campaigns.
  University of Maryland, School of Medicine,
  MedSchool Maryland Productions.
  Baltimore, Maryland.

- June 2012 - Present.
  Freelance Multimedia Designer.
  Kellie Gable Design.
  Baltimore, Maryland.

- January 2013 - October 2014.
  Web Designer.
  A&A Global Industries.
  Cockeysville, Maryland.

- April 2012 - December 2012.
  Advertising Art Director.
  Raffiné Media.
  Stevensville, Maryland.

- August 2011 - June 2012.
  Email Marketing Specialist.
  Allegis Group.
  Hanover, Maryland.

- May 2010 - August 2010.
  Art Intern.
  Baltimore Magazine.
  Baltimore, Maryland.

- August 2009 - May 2012.
  Resident Assistant.
  Stevenson University.
  Owings Mills, Maryland.

ABSTRACT

Title of Document: EXPLORING OLDER ADULTS' ATTITUDES TOWARDS PRIVACY OF ADAPTIVE ASSISTIVE TECHNOLOGIES.

Kellie Nicole Gable Poneres, Master of Science, 2018.

Directed By: Dr. Aaron Massey (Chair)
Dr. Foad Hamidi
Dr. Amy Hurst

Adaptive assistive technologies can support the accessibility needs of individuals whose abilities vary due to a diagnosis, medication, or other external factors by monitoring and adapting to their fluctuating performance. As these systems offer many compelling benefits to users, the privacy threats posed by these systems has been largely overlooked in Human-Computer Interaction (HCI) literature. This work identifies potential privacy threats posed by adaptive assistive technologies, and investigates the privacy-related perspectives and concerns of older adults who experience varied pointing abilities, in the context of these systems. In our first study, we conducted eight interviews with older adults diagnosed with Essential Tremors. Six months later, six of our participants partook in novel participatory privacy elicitation activities in the second study. We found that participants had positive attitudes towards assistive technologies that gather

their personal data, but also had strong preferences for how their data should be used and who should have access to it. We identify a need to factor in privacy threats when designing assistive technologies to avoid exposing users to these hazards. We conclude with design recommendations to offer users more agency over their collected data from these systems.

Acknowledgements

I am fortunate to have had an invaluable academic experience fostered by my knowledgeable and passionate instructors at UMBC. I offer my deepest thanks to my primary advisor and mentor, Dr. Foad Hamidi, for introducing me to the exciting world of research. Your guidance, knowledge, patience, and enthusiasm has truly been instrumental in my learning process and passion for research. I would also like to thank my secondary advisors and mentors, Dr. Amy Hurst and Dr. Aaron Massey. Amy's devotion to accessible technology research and ability to approach research from a creative lens, has been a tremendous contribution to my growth and research initiatives. Dr. Massey's knowledge and enthusiasm for privacy-related research and standards, interest in inclusive privacy, and valuable input has tremendously contributed to my academic success.

To my husband, αγάπη μου—Your unwavering support has been an immense source of encouragement and comfort throughout my graduate career. Thank you for adding comic relief to the many late study evenings. Your radiant positivity is always appreciated.

Table of Contents

List of Tables

List of Figures

1 Introduction: Exploring Privacy and Adaptive Assistive Technologies

Introduction and Overview

Adaptive assistive technologies (AATs) hold the potential to deliver promising accessibility solutions to users who experience varied pointing ability, attributable to a medical diagnosis, medication, or other external factors [91, 44, 39, 40]. Existing Human-Computer Interaction (HCI) literature pertaining to adaptive assistive technologies is predominantly focused on the improvement of system interfaces [31, 33], and exploring potential benefits users can obtain through adaptation of these systems [91, 44, 39, 40]. However, as existing HCI literature has placed focus on the many ways these systems can support accessibility needs, there has been limited research evaluating adaptive assistive technologies in the scope of privacy.

As a growing number of individuals may be incentivized to adapt these systems to reap prospective performance benefits, we address the acute need for investigation into potential privacy threats posed by adaptive assistive technologies. In this research, we contribute to the growing body of HCI literature by addressing the overlooked issue of privacy in the context of adaptive assistive technologies. We initiate exploration into the unexplored role of privacy in adaptive assistive technologies by identifying potential privacy threats posed by these systems, and examining privacy-related perspectives and concerns of older adults who experience varying pointing abilities. To facilitate future research in this domain, we introduce a novel methodology for exploring privacy-related perspectives, in the context of adaptive assistive technologies, within a designated subpopulation.

Elements of this research have recently been published as a peer-reviewed technical paper and poster in the *Proceedings of the 20th International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS 2018)* [30, 76]. This thesis expands on the previous published work with a follow-up study yielding additional in-depth insights into older adults' privacy concerns surrounding adaptive assistive technologies.

Thesis Motivation

Adaptive assistive technologies are defined by their ability to autonomously modify their functionality to adapt to a user's performance and goals, through the collection of user data [81, 44, 30, 39]. These systems pose benefits to users by facilitating increased performance and task regulation through the reduction of user errors [73]. Beyond providing advantages for general usage, adaptive assistive technologies can help older adults who experience intermittent or gradual changes in pointing ability due to health conditions, such as Essential Tremors (ET), Parkinson's Disease, arthritis, or fatigue [91, 44, 39, 40]. As motivation and perceived need for adopting these technologies may be greater for this population, it is necessary to explore older adults' values and perspectives in regard to their use of adaptive assistive technologies. We intentionally recruited individuals who experience variable, mild, or non-impeding difficulties because they might be more sensitive towards disclosure of their health information than people who had been diagnosed with more severe and permanent disabilities. Many of our participants had been diagnosed with Essential Tremors but did not identify as being "disabled" and were dealing with the emotional and practical impact of experiencing difficulties due to changes in

abilities. Essential Tremor (ET) is a chronic, progressive neurological disease whose defining feature is kinetic tremor of the hand and arms [56]. It is known to negatively impact employment with 15-25% of people with ET retiring prematurely, and 60% choose not to apply for a job or promotion because of uncontrollable shaking [8, 78]. ET is currently the most prevalent form of movement disorder in the world [57].

Increasingly, adaptive systems are connected to online servers that allow for the remote monitoring of user activity, as well as the collection and aggregation of user data to improve overall system functionality. While the shift towards connectivity and increased data collection presents opportunities for system performance improvements, it can also expose users to privacy vulnerabilities and threats. This issue is amplified as the data collected by assistive applications might intersect with sensitive personal health information, yielding the potential risk of undesired medical disclosures [100].

Recent research has identified many online privacy threats when users' personal data is accessed and collected by remote platforms [5, 85, 89]. Alarming news stories have reported the abuse of users' personal data by companies (e.g., the 2018 misuse of user data on the Facebook social network by the Cambridge Analytics company in which the data of approximately 50 million users were accessed by a 3rd party company [80], as well as security breaches leading to the leaking of sensitive data to unknown parties (e.g., the 2017 Yahoo! security breach in which hackers obtained access to the email accounts of allegedly 3 billion users [24]). In addition to these large-scale data breaches, other privacy threats are emerging with the development of automatic mechanisms for the early detection of health conditions, including neurodegenerative diseases, from users' online behavior. In a recent study, White et al. utilized search input from

more than 31 million users to develop a machine learning algorithm to detect early signs of Parkinson's disease and Alzheimer's disease from users' online search data [100]. This research and similar efforts that analyze keyboard [23] or touchscreen input [6] to detect disease have mostly focused on the technical aspects of the systems. Their development, however, raise serious questions about user privacy [79].

Several organizations, such as the Citizen Lab (citizenlab.ca) and the Electronic Frontier Foundation (eff.org) are raising the public's awareness of the nature and frequency of the privacy threats users face online. These efforts make it clear that user privacy is increasingly important to consider when designing *any* system that collects user data. However, security and privacy are rarely discussed within the accessibility research and design communities, and vice versa. While designing for privacy is difficult and not commonly done [29], this omission is problematic as users who use assistive technology might be especially vulnerable to data breaches. For example, individuals who exhibit changing abilities, due to age or disabilities, might experience severe consequences in their job or insurance status based on disclosure of a potential diagnosis [8, 78]. These users may not be aware of the blurry line that exists between medical applications that adhere to privacy standards and independently developed assistive systems that increase accessibility but do not provide the same privacy practices. According to the U.S. Health Insurance Portability and Accountability Act (HIPAA), healthcare information is only protected when provided to a defined covered entity for medical purposes [95]. Information provided to an assistive technology company or available to websites or other third parties– including information that clearly reveals particular healthcare concerns–is not protected. Thus, it is

possible that users are not aware of the privacy threats that might exist when choosing online assistive technologies.

In summary, our team was motivated to conduct this research to address the overlooked element of privacy in the context of adaptive assistive technologies. The current climate of increasing online personal data violations, lack of investigation into potential privacy threats in adaptive assistive technologies, and failure of existing HCI research to address vulnerable populations' attitudes towards privacy when using these systems have propelled our research endeavors.

Research Questions

The primary motivation for this research was to learn *what are users' perspectives, attitudes, and concerns towards privacy in the context of adaptive assistive technologies?* In order to address our primary research question, we developed two associated, minor research questions. Our second associated research question aimed to contextualize users' concerns by identifying some of the privacy threats that users of adaptive assistive technologies are exposed to. Through our third associated research question, we endeavored to learn how researchers can use participatory methodologies to elicit privacy attitudes from end users.

Research Question 1: What are users' perspectives, attitudes, and concerns towards privacy in the context of adaptive assistive technology?

While literature on adaptive assistive technologies is robust, users' privacy concerns when interacting with these systems has been largely overlooked in Human-Computer Interaction

(HCI) literature. Our main objective in conducting this research is to address this omission by answering our primary research question: *What are users' perspectives, attitudes, and concerns towards privacy in the context of adaptive assistive technology?* This question is paramount to our investigation, as we must learn users' attitudes and perceptions towards privacy to make informed privacy-minded recommendations for designers of adaptive assistive systems. Due to the fact that users of these systems could be at risk of unwanted data disclosures and other alarming privacy threats, we assert the significance of exploring users' attitudes towards privacy when using these systems. We were distinctly interested in exploring the privacy concerns of individuals who may be more vulnerable to privacy threats when interacting with these systems.

Research Question 2: What privacy threats are users of assistive technologies exposed to?

Our second associated research question aimed to contextualize users' concerns by identifying some of the privacy threats that users of adaptive assistive technologies are exposed to. We aimed to examine *What privacy threats are users of assistive technologies exposed to?*, to gain insight into our first research question and frame our participant interview data analysis.

Research Question 3: How can researchers use participatory methodologies to elicit privacy attitudes from end users?

Our final associated research question derived from our interest in gathering thorough data pertaining to our first research question. We inquired *How can researchers use participatory methodologies to elicit privacy attitudes from end users?*, to develop novel privacy elicitation methods to procure more extensive data from our participants.

Contribution

This research offers a series of contributions to the growing body of HCI literature focused on adaptive assistive technologies. First, we provide insights into user perceptions, attitudes, and concerns towards privacy in the context of an adaptive assistive technology probe. We advance and contribute to the third wave of privacy and security, inclusive privacy, by conducting our research with an underrepresented subpopulation-- older adults with Essential Tremors. Next, we present and apply a meta-analysis of a privacy threat model to adaptive assistive technologies, and use this model to identify and categorize general privacy threats that might arise from their use. Third, we introduce a novel participatory methodology for eliciting privacy attitudes, in the context of adaptive assistive technologies, within a designated subpopulation.

Finally, we offer design recommendations for developers and hosting sites of adaptive assistive technologies. The first design recommendation features a custom-designed icon set, representing seven key privacy features, to inform users about the privacy and data-collecting nature of an adaptive assistive technology. The second design recommendation presents a data privacy settings page, designed to further inform users and give them agency over their data collected by adaptive assistive systems.

Our first two contributions provide a better understanding of the types of privacy threats involved in using assistive technologies and users' perceptions and attitudes towards them. We believe that these results underline privacy questions that need to be considered when designing *any* assistive technology that collects user data to improve its usability and functionality. Our

other contributions aim to give designers tools to improve the usable privacy of adaptive assistive technologies.

2 Related Work

While literature on adaptive assistive technologies is robust, the privacy threats posed by these systems has been largely overlooked in Human-Computer Interaction (HCI) literature. Furthermore, we conducted a search of the Association for Computing Machinery (ACM) Digital Library to examine the breadth of existing research related to adaptive assistive technologies. As of November 2, 2018, a search for phrases matching "adaptive assistive technologies" in publication abstracts yielded 240 results. However, on the same date, a search for words matching "adaptive assistive technologies privacy" in publication abstracts yielded only five results. It must be noted that two of these five results were publication products of our team's research, referenced in this thesis. In the three remaining paper abstracts, emphasis was placed on the unique functionality and design attributes of featured adaptive assistive technologies, where *privacy* was included to describe privacy-conscious design features in the systems. Although a small number of publications considered user privacy in the design of adaptive assistive technologies, there has not been research dedicated to the exploration of privacy threats in these systems or users' privacy concerns when interacting with these systems. We maintain the importance of investigating adaptive assistive systems through the lens of privacy, for users of these systems could be at risk of unwanted data disclosures and other alarming privacy threats.

Privacy in Information Technologies

In 1967, Alan Westin offered a definition of *privacy,* in the domain of information technology, which can be summarized as personal control over one's data, extending to control over the extent and manner in which that data is accessed and shared [99]. Nearly a decade later, Irwin Altman shared this control-centric notion of privacy, but added that privacy is both a social and psychological process in which individuals can regulate boundaries in social interaction and personal space [4, 49]. Jim Harper expanded on this idea of control as the driving force behind privacy, by adding that it is not the mere act of exercising control over one's personal data, but how an individual *feels* when they are empowered to exercise that control [34]. Many definitions of privacy have surfaced, yet no definition has been unanimously revered as the superior, all-encompassing definition of privacy [69].

In our work, we embrace an inclusive definition of privacy that acknowledges the degree to which one is able to exercise agency over their personal data, the emotions one experiences when defining and adhering to boundaries with their personal data, and that both privacy-related agency and emotion are uniquely experienced by the individual. The concept of *privacy* is inherently subjective, as individuals hold varying interpretations and emotional responses regarding the significance of privacy in different online contexts [49, 34]. As information technology further develops, the concept of privacy, and attitudes towards the impalpable entity evolve within this domain.

Often, software development organizations struggle to implement proper privacy principles into their system design process [28]. Additionally, information technologies are typically designed to meet the privacy needs of the general population, rather than the unique needs of established sub-populations [98]. These two combined issues of failing to properly weave privacy by design into the system design process [3] and favoring privacy design solutions geared towards the masses, can result in software systems that discount and neglect the privacy needs of marginalized populations. This in turn renders these groups more susceptible to privacy and security vulnerabilities when interacting with new technologies. Inclusive privacy advocates for technology systems that are designed to meet the privacy and security needs of individuals with distinct abilities, perspectives, and needs [98]. By initiating research on privacy attitudes and perspectives within underrepresented subpopulations, we can develop more effective human-centered privacy design solutions in the future. The significance of HCI exploring privacy expectations of vulnerable populations is to prevent negative outcomes perpetuated by modern non-inclusive design solutions in software systems.

Essential Tremors (ET)

We have chosen to focus on the privacy attitudes and perspectives of older adults with Essential Tremors. Essential Tremors (ET) is a chronic, progressive neurological disease, manifesting as a kinetic tremor [56, 57]. Nearly 7 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 [58]. Despite the prevalence of ET, there is little representation of this subpopulation in research under the context of privacy in information technology. ET is

known to negatively impact employment in the form of premature retirement and individuals opting to forgo application for a promotion or new job opportunity because of uncontrollable shaking from tremors [8, 78].

User Perceptions and Concerns about Online Privacy

There is a growing body of research on end user perceptions and attitudes towards privacy tradeoffs of online applications [5, 10, 43, 85, 107]. Most of these projects focus on online marketing [5, 85] and IoT and wearable applications for health [25, 107]. Several studies found that 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 [5, 85]. 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 [5]. Additionally, there may be a mismatch between users' mental models and how personal data is actually collected and used. This mismatch can lead to unpleasant surprise and discomfort when users are informed [10, 25, 43, 107]. 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 [71].

Several projects have studied the privacy tradeoffs of health monitoring and location sensing systems for older adults [63, 97]. McNeill and colleagues conducted interviews with 20 older adults about their privacy concerns with pervasive health-monitoring systems [63]. They found that privacy was valued by their participants and important to their sense of life fulfillment. 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 [63]. 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 [50, 51]. Given the complexity of the choices faced by stakeholders when choosing these systems, previous research has called for nuanced studies to help designers understand the multifaceted socio-technical issues involved in designing and deploying these systems [16, 97]. More broadly, researchers have recommended the development of multifaceted strategies that combine technical, legal and social mechanisms to develop "privacy-friendly" personalized systems [48, 52], including IoT systems for people with disabilities [37].

Adaptive Assistive Technologies to Support Pointing Performance

Changes in pointing ability can occur due to a range of factors, including advanced age [14, 38, 44, 46, 64, 91, 101, 104], a temporary or sustained disability [84, 93, 103] and medical conditions such as Essential Tremors (ET), Parkinson's, arthritis, or fatigue [44, 70]. These changes can make computer use difficult [14, 27, 44, 70]. In some cases, individuals are unaware of the cause of their input errors [64, 65] or changes in their abilities [13]. Moffatt's studies of pen-based menu selection tools revealed that users of their system were often unaware of the cause of their difficulty selecting menu items and why unintended menu items opened [65]. Other individuals are aware of changes in pointing ability, but these changes occur with unpredictable frequency and severity [87, 92].

Several *adaptive* (or *personalized*) *assistive systems* have emerged in the last decade to support individuals with dynamically changing pointing abilities. These systems provide assistance by changing their functionality or appearance based on user activity, the state of a system, or both [31, 70, 81]. They are built on platforms that automatically detect changes in pointing performance as an individual uses a pointing device to interact with a computer (e.g., [39]). Several systems have specifically focused on helping users with pointing challenges that impact target acquisition [38, 103] and target selection [3, 81, 93, 105]. These systems help improve a user's ability to use an input device to select interface elements (e.g. clicking on buttons, positioning the cursor). Other projects have focused on understanding the concerns and expectations of users of adaptive systems with respect to information they would like to receive during interaction [31, 33]. To date, researchers have not examined the privacy threats that might arise from using AATs or the perceptions and attitudes of end users towards these issues.

Plutchik's Wheel of Emotions

Plutchik's wheel of emotions has been used as framework for identifying emotional sentiment in Human-Computer Interaction research [60, 21, 82]. The emotion wheel presents a categorical representation of 32 emotions strategically formatted onto an annular model [74,75]. The middle ring holds, what Plutchik identified as, the eight primary emotions. Plutchik theorized that the remaining emotions are related to the primary emotions, by increasing or decreasing the intensity of those emotions [75]. Variant emotions with increased intensity are placed in the innermost ring, while less intense derivative emotions are placed further away from the core.

Koto and Adriani [60] used Plutchik's eight primary emotions as framework for developing an emotion lexicon from Twitter data. Runge et al. built a user interface abstraction of Plutchik's wheel, dubbed *the EmoWheel*, to facilitate image tagging on mobile devices [82]. Franzoni et al. utilize the emotion models of Plutchik, Ekman, and Lovheim to develop a semantic model for measuring the emotional load of specified web objects [21].

3 LINDDUN: Identifying Privacy Threat Framework for Input-Based Adaptive Assistive Technologies

In this chapter, we investigate the scope of potential privacy threats for end users interacting with adaptive assistive technologies (AATs) with a meta-analysis of the LINDDUN threat modeling framework's six threat categories [17, 106]. Applying the threat modeling framework to adaptive assistive technologies allowed us to gain insight into our second research question (*What privacy threats are users of adaptive assistive systems subjected to?*), as well as frame our participant interview data analysis.

Threat modeling is a process for discovering, classifying, and evaluating the risk of threats from an attacker's point of view. Originally, threat modeling was exclusively used for information security purposes. Microsoft's STRIDE classification serves as an exemplar [86] to provide guidance to analysts regarding what parts of the system to examine and how to do the examination. Applying STRIDE produces a classified set of threats for an application from the perspective of a defined attacker with known goals.

Privacy researchers have extended threat modeling to address privacy concerns too nuanced to be directly addressed by security-oriented approaches. In this paper, we examine the LINDDUN threat modeling framework [17, 106], which is analogous to STRIDE and provides similar guidance to uncover privacy threats. LINDDUN is an acronym that represents Linkability, Identification, Non- repudiation, Detectability, Disclosure of information, Unawareness, and Non-compliance. As with STRIDE, LINDDUN can only be formally applied to concrete systems with defined software artifacts, including requirements and a data flow diagram (DFD).

Application: Applying LINDUUN Framework to Adaptive Assistive Technologies

We framed the LINDDUN threat modeling framework in the context of AATs that collect and analyze a user's pointing or typing data to assess ability and (potentially) deploy custom assistance. This class of technology includes software that tracks pointer, touchscreen, or typing use to assess performance in a browser or at the operating system level [6, 22, 39, 31, 100]. While we have focused on AATs, many of the discussed points are also relevant to consider for other assistive technologies including screen readers, AAC devices, and voice transcription software that are used on an internet-connected device.

Linkability

Linkability refers to the ability of data to be linked to another item of interest without directly identifying information (e.g., names or created identifiers). For example, if an AAT collects input data that can be definitively linked to a particular healthcare diagnosis (e.g., by using algorithms that detect early signs of Parkinson's disease [100]), that represents a threat in the linkability classification. A concerning example would be an employer exploiting the detectable presence of an AAT for pointing in a job applicant's web browser to screen out potential applicants. Linkability only requires the presence of an AAT and the implication that it is used to address a healthcare concern. No direct identifiers are present or even needed to make this connection for someone applying for a job through a web-based portal.

Identifiability

Identifiability threats allow for easier or more direct identification of individuals within a larger set of anonymous subjects. In the trivial case, an AAT that embeds personally identifying information into its usage data would be directly identifiable for a user. A more complex potential example would connect data patterns of a system running an AAT over time to serve as a means of identification. This example represents browser fingerprinting [2, 67], an identifiability threat where unique browser preferences, customizations, and capabilities can be connected across prior visits to a given website. Depending on the uniqueness of the AAT, even having this technology installed and disabled may provide information that can contribute to a fingerprinting algorithm. Finally, the analysis of a user's anonymous input data may reveal their identity. Past research has demonstrated the potential for this through analyzing the idiosyncratic patterns of individuals typing on keyboards as a biometric authenticator [66].

Non-repudiation

Non-repudiation threats refer to the prevention of plausible deniability as a part of an individual's privacy controls. For example, if a website can produce irrefutable evidence that a user must have been the one to perform an action (e.g., browsing a website, uploading a photo, or writing a comment) because of the use of an AAT, then the pool of other plausible options is potentially eliminated. Depending on the data provided by the tool, the use of, or perhaps even presence of, an AAT can limit the extent of a user's plausible deniability. As with other LINDDUN threat categories, the extent to which threats of this nature are dangerous depends on the tool. Most other assistive technologies in web-based applications are detectable by the browser, and some

may be detectable by browser plugins (depending on the level of access provided and the browser). For example, a server or website's ability to detect the use of Accessible Rich Internet Applications (ARIA) [96] attributes to surreptitiously collect usage data that would constitute a non-repudiation threat remains, in general, unexamined.

Detectability

Detectability refers to the ability of an attacker or outsider to detect the existence of an item of interest. Detecting if a user is actively using an AAT serves as an example of this threat. This threat can lead to unwanted disclosure of a disability which makes it a key threat to consider in this context. This threat is especially serious for users who are starting to experience changes in their abilities and whose employment or insurance status might be impacted by unwanted parties learning of these changes. AATs that monitor user performance and can detect changes over time pose this threat (e.g., [31, 100]).

While clearly problematic, active detection as explicit bias might not be the most challenging way detectability threats manifest themselves. Consider implicit algorithmic bias where the data used to train an AI simply defines "normal" using a dataset that does not fully or fairly represent the actual population [47]. Modern AIs are extremely good at detecting deviations in behavior patterns, but they do not know if those deviations are "fair" or "unbiased." If such algorithms are applied widely to analyze website interaction and detect deviations from the majority of interactions, they can pose further threats to users of assistive technologies. Disclosure of Information LINDDUN describes disclosure of information as the straightforward release of

information to anyone not authorized to see it. In general, this threat category is unlikely to be a primary driver of privacy threats for most assistive technology users because they do not currently store or rely on a great deal of sensitive information to operate. Other privacy threat categories that depend on linking or inferring data are more likely to pose direct privacy threats. However, this threat is more significant for AATs that collect user performance data over time and may sync settings and usage data across multiple machines. Any accidental release or access of this data by an unauthorized party would fall into this privacy threat category. Depending on the nature of the data, a breach could reveal precise information about an individual's pointing ability (and efficiency) and the severity, or onset, of a pointing problem.

Unawareness

Unawareness refers to an end user not understanding the consequences of sharing personal information. Unfortunately, prior research indicates this privacy threat category is likely to be a serious concern for many individuals. Documents describing data sharing practices are difficult to read, resulting in few users willing to read them [61]. When users do read these documents, they systematically misunderstand their implications for data sharing [18]. The result of the so-call "notice and choice" approach to privacy is that users simply fail to understand the implications of modern advertising data practices [62]. To our knowledge, no published research exists assessing whether these prior research findings also hold for AAT users, however, we posit that it is unlikely that the notice and choice approach is effective for this user group. Another unawareness concern is the data collected and shared by the assistive technologies that users are currently using. AATs may collect, aggregate, and share data to identify improvements for tool

performance and user preferences. This information may be sensitive, depending on the context and the tool, and users may be unaware of this collection.

Non-Compliance

Privacy threats related to non-compliance are characterized by a failure to comply with laws, regulations, and corporate policies. This category of threats is uniquely applicable to AAT target users, many of whom are protected by accessibility regulations. Unfortunately, compliance with accessibility regulations is as difficult to engineer as other regulations governing broad societal goals [13] and may not provide privacy protections. In fact, accessibility regulations may require disclosure of information that would itself be concerning for users of assistive technologies. In all other respects, however, users of AATs are roughly as likely to be as vulnerable to Non-Compliance privacy threats as most other users of technology.

4: Methods

The current chapter details our experimental approach and methodology used during this two-part study. It is organized into two main sections: Study 1 - Exploring Attitudes Towards Privacy with Interviews and a Design Probe; Study 2 - Participatory Privacy Elicitation Activity. Both studies were conducted to answer our first primary research question: *What are users' perspectives, attitudes, and concerns towards privacy in the context of adaptive assistive technology?* The second study aimed to answer the primary research questions by employing novel participatory methodologies and subsequently answering our third associated research question: *How can researchers use participatory methodologies to elicit privacy attitudes from end users?* Both main sections are parsed into five subsections: Study Design; Participant Recruitment; Limitations; and Data Analysis.

Study 1: Exploring Attitudes Towards Privacy with Interviews and a Design Probe

To contextualize and understand user attitudes towards privacy of adaptive assistive technologies, we conducted interviews, centered around an adaptive assistive technology design probe, with eight older adults who experience variable pointing problems due to Essential Tremors. The following *Study Design* subsections detail the *Interview Design* and *PINATA Adaptive Assistive Technology Design Probe* attributes and design processes.

Interview Design

We conducted a user study with eight semi-structured in-person interviews. The primary reason for opting to host in-depth, in-person interviews with a smaller sample size was rooted in the objective of gathering rich qualitative data about our participants to focus on understanding the context [77] of privacy in the aforementioned domain. The flexible and exploratory nature [77] of the semi-structured interview format would allow participants to detail their experiences and perception of privacy with online adaptive assistive technologies, offer anecdotes of these experiences, and discuss the role their health condition may have had in these events.

Our interviews focused on experiences using technology, and perceptions of privacy online (with and without assistive technologies). The protocol began with demographic questions, including the history, nature, and frequency of participants' pointing difficulties. This included their past and present computer use and their employment and career histories. We also asked participants if and how the pointing difficulties they experience impacted their computer use at previous jobs or currently impacted personal use. These questions helped us understand participants' motivations for using the Internet and the range of applications that were important to them.

Demographic questions were followed by questions about the participants' experiences with online adaptive systems. We chose examples that were not overtly designed as assistive technologies (e.g., the Amazon ecommerce website). If participants offered examples of their own, we would ask them to elaborate on these scenarios rather than our examples. We asked

participants about any concerns they have with respect to how their data is used by these systems and to what extended they trusted them.

We then showed PINATA to the participants, as an example of an adaptive assistive technology that can help them with pointing tasks. We informed the participants that no pointing data was collected during the interviews. In addition to showing and describing how the system works, we asked them to interact with its different components. We asked participants to move the system's *dynamic bubble cursor* using a pointing device of their choice (e.g., a mouse or trackpad) to select links on a couple of example website (Figure 1). Additionally, we asked them to hover and click over the different parts of the *pointing history browser* (Figure 2) to access visualized sample pointing performance information. We then asked participants about their input on these components and the overall system functionality.

The interviews were conducted in a semi-structured interview format, composed of a defined script, and predetermined closed and open-ended questions. This format was employed to elicit consistent, relevant qualitative data while creating opportunity for participants to provide related data [77].

To view the finalized Study 1 protocol, please refer to Appendix A.

PINATA: Adaptive Assistive Technology Design Probe

We developed a functional prototype of an adaptive assistive technology, *Pointing Interaction Notifications and AdapTAtions* (PINATA), for participants to interact with. PINATA monitors

users' pointing performance when accessing the Internet and dynamically adjusts the size and selection area of the on-screen cursor in response to pointing difficulties. PINATA is implemented as a Chrome extension that can be installed in a users' browser and assist selecting on-screen elements.

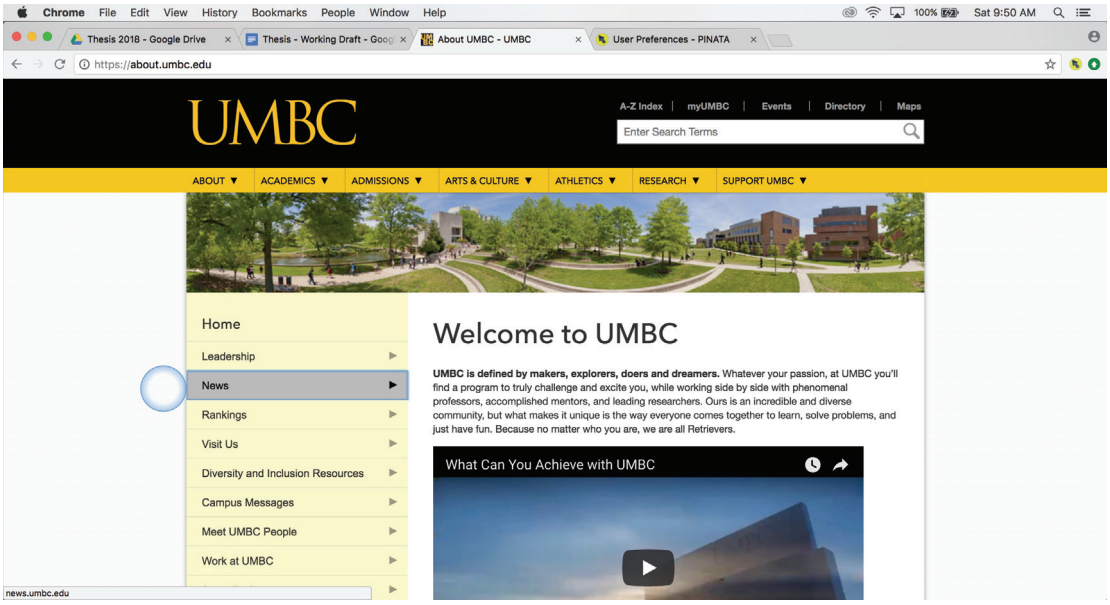


Figure 1. PINATA's adaptive bubble cursor. The adaptive bubble cursor's selection area expands in response to an increase in detected pointing errors. The larger size of the selection area facilitates ease in target selection for users.

The system consists of several modules. The main pointing assistance is provided as a dynamic *bubble cursor* (Figure 1). A dynamic *bubble cursor* is a modified cursor that has a larger selection area than the default cursor that dynamically changes size as the cursor gets closer to selectable objects. In previous research, it has been shown to support efficient target selection for users with and without disabilities [20]. We chose a dynamic bubble cursor as the assistance presented to users because it provides contextual visual feedback to users (a circled area around the cursor), while not impacting the visual appearance of the underlying website. These features are previously found to be desirable by users of adaptive assistive interfaces for web navigation [31, 33].

The bubble cursor could be deployed in two modes: *automatic mode* where it monitors user performance and adjusts its size accordingly, or *manual mode,* where it is only activated if a user decides to change the settings themselves. In the automatic mode, the assistance can also be deactivated if improvements in pointing performance are detected over time. The functionality and appearance of the bubble cursor can be adjusted by a *user preference manager*. This part of the system allows users to specify if assistance should be deployed manually or automatically, if and how frequent contextual notifications should be provided when performance difficulties are detected, and the shape and color of the bubble cursor.

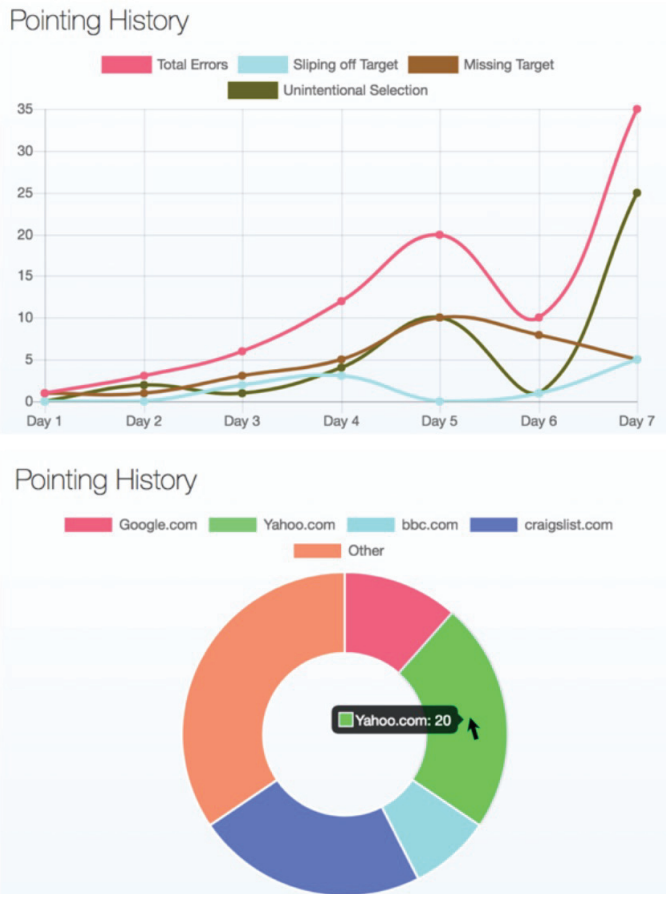


Figure 2. PINATA's pointing history visualizations. The pointing history visualizations depict pointing error data to the user in two graphs: the *Error Type Graph* (top) and the *Website Graph* (bottom). The *Error Type Graph* depicts the frequency of different types of errors over time, while the *Website Graph* depicts the most frequent websites where pointing errors have occurred.

The *pointing history browser* (Figure 2) visualizes pointing data that could be collected from the users. These include the frequency and type of pointing errors detected over time and the most common websites that where the errors occurred. In this study, the visualized data was not collected from the participants' interactions and was created to give the participants a sense of the type and amount of data that could potentially be collected by PINATA. To ensure privacy, our software did not collect any performance or usage data during the study.

Participant Recruitment

We recruited eight older adult participants, age 65 years or older, who experience different frequencies of pointing difficulties (Table 1). Most participants were recruited from a local organization providing support to individuals who experience Essential Tremors (ET). We chose to work with this population because the effects of Essential Tremors happen gradually and can impact employment and access to computers adversely [8,78]. Because of these conditions, individuals experiencing Essential Tremors may be reluctant to disclose their health information to employers or insurance companies and may be motivated to adopt assistive technology that helps them compensate for their changing abilities. The study was conducted in the context of a large metropolitan city in the United States.

Seven participants experienced difficulties due to ET and one participant experienced difficulties due to vision impairments (P6). At the time of the study, every participant reported experiencing intermittent difficulty when using a pointing device, and none reported impairments that would completely impede computer use.

All participants considered themselves to be retired at the time of the study (except for one who was employed part-time) had experience using computers in their previous careers and subsequently in their retirement. All participants expressed pointing difficulties with one or more of the following pointing devices; computer mouse, trackpad, and/or touchscreen. Some of the most frequently-experienced pointing difficulties included clicking on target items, maintaining a steady hand while navigating, overshooting or missing the on-screen target, slipping off an item when clicking, and losing the cursor. Participants indicated fluctuating pointing performance dependent upon time of day, fatigue, caffeine intake, exercise, alcohol intake, and/or heightened emotions.

ID	Age	Gender	Career History	Reason for Pointing Difficulty	Weekly Internet Use (Hours)	Perceived Value of Internet
P1	71	Female	Customer Service	Essential Tremors	2 Hours	Somewhat Valuable
P2	82	Male	Forestry	Essential Tremors	25-30 Hours	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	77	Female	Educator (Elementary and Special Education)	Vision Impairment (Cataracts)	7-14 Hours	Very Valuable

P7	73	Male	Educator (University)	Essential Tremors	14-28 Hours	Very Valuable
P8	82	Female	Librarian, Massage Therapist	Essential Tremors	18-21 Hours	Very Valuable

Table 1. A table summarizing the demographics and backgrounds of participants from Study 1. Participants were given alphanumeric IDs based on the chronological order in which they participated in Study 1 (i.e P1 represents the first participant, while the last participant is labeled P8). The participants' age, gender, career history, reason for pointing difficulty, reported weekly internet use in hours, and perceived value of internet access are included in the table. All participants considered themselves retired with the exception of P1, who described being employed part-time.

Limitations

As this exploratory study marked our initial investigation into older adults' attitudes towards privacy of adaptive assistive systems, we chose to host in-depth semi-structured interviews to gather rich qualitative data. The pitfalls of employing the in-person interview methodology include the time-intensive nature of the activity, and that the data is by no means generalizable to all older adults experiencing variable pointing difficulties [77]. Limitations in generalization should also be taken into account for our small sample size of eight individuals. Additionally, our interviews focused on first impressions about privacy threats when interacting with adaptive assistive technologies, as the participants had limited time interacting with the design probe. After demoing PINATA, the participants described their privacy concerns with the application. Furthermore, we believe participants' responses to be limited to their brief interaction with the design probe, and could evolve with extended use of the program as users' attitudes change with continued use of technology [9].

Data Analysis

We audio recorded and transcribed each interview, with the exception of one interview (P4), in which we took detailed notes instead at the participant's request. Once the interviews had been transcribed, the data was formatted into an Excel spreadsheet and color coded based on participant responses (Figure 3) to create an aggregate data visualization. The color-coded presentation of the aggregate data visualization allowed us to quickly identify high-level patterns amongst our participants, and compare and contrast their responses.

	P1	P2	P3	P4	P5	P6	P7	P8
Gender	Female	Male	Male	Male	Female	Female	Male	Female
Age	71	82	69	87	64	77	73	82
Employment BG	Customer Service	Forestry	Geology/ Computer Tech, Army, Peace Corps	Airforce; Pilot, Accountant, Computer Specialist	Computer Systems Analyst, Fitness Tech, Stay-at-Home Mom (first few years)	Education; Elementary Teacher, Educational Coordinator, Teacher for DOD, Special Education	Education; University Instructor	Librarian and Massage Therapy
Currently Employed?	Yes - Part-Time (1 Day per week)	No	No- Volunteers & Consults	No	No	No	No	No
Retired?	Yes	Yes	Yes	Yes >30 years	Yes	Yes since 94'	Yes	Yes
Regularly use desktop?	No	Yes	Yes	Yes	Yes	Sometimes	No	Yes
Use desktop w/ internet?	No	Yes (but mostly on phone)	Yes	Yes	Yes	Yes	No	Yes
Regularly use Laptop?	Yes	No	Yes	Yes	No	Yes	Yes	No
Use laptop w/ internet?	Yes	No	Yes	Yes	No	Yes	Yes	No
Regularly use touch-based tablet?	Yes (iPad)	Sometimes/Rarely	Yes (iPad)	No	Yes (iPad & Kindle)	No	Yes (Samsung)	No
Use tablet w/ internet?	Yes	Sometimes/Rarely	Occasionally	No	Yes	No	Yes	No
Regularly use Smartphone?	No	Yes (Apple)	Yes (Android)	No	No (owns one, but prefers not to use it)	Yes	Yes (iPhone)	No
Use smartphone internet?	No	Yes	Rarely	No	No	Yes	Yes	No
Regularly use other Cell Phone?	Yes	No	No	Yes	No	No	No	Yes
Use internet on other cell phone?	No	No	No	No	No	No	No	No
Regularly use mouse?	Yes (Wireless)	Yes	Yes	Yes	Yes	No	Yes	Yes
Regularly use touch screen?	Uses Stylus on iPad (avoids touch)	Yes (Phone)	Yes (iPad)	No	Yes (iPad & Kindle)	Yes	Yes	No
Regularly use Trackpad?	No	No	No	No	No	Yes	Less Regularly	No

Figure 3. Study 1 color-coded aggregate data visualization. The participants are defined in the columns, while the interview questions define the rows. Colors were given to responses (i.e. Green=Yes, Red=No, Orange=Sometimes/ Maybe) to support pattern and theme identification amongst participants.

To further distill the data, we conducted an iterative thematic analysis to identify and synthesize themes [11] within the transcriptions. Kellie Gable transcribed the interviews, introducing an initial stage of coding. This included noting keywords, prominent emerging themes, supporting anecdotes, and patterns in the margins of the transcripts. Dr. Foad Hamidi and Dr. Amy Hurst

then added a second layer of coding which consisted of further analysis and theme identification. Once the second coding phase had been completed, we then met in-person and discussed the data in extent, further refining our theme classification as a research team.

Study 2: Participatory Privacy Elicitation Activity

To further contextualize and understand user attitudes towards privacy of adaptive assistive technologies, we developed a privacy elicitation activity which we then conducted with six of our participants from Study 1. Study 2 was conducted approximately six months following Study 1. The main intent behind Study 2 was to compare participants' privacy preferences between assistive typing and assistive pointing applications, test the newly developed privacy elicitation activity, collect more extensive data, and to identify if there were any changes in participants' attitudes and perspectives towards privacy of adaptive assistive technologies since Study 1. The following *Study Design* subsections detail the *Materials* and the *Participatory Privacy Elicitation Activity Design* components of Study 2.

Materials

We developed several physical paper components for the Participatory Privacy Elicitation Activity. These components consisted of printed Scenario Cards, Data Type Cards, Party Cards, the Expectations Chart, the Emotion Wheel, and Privacy Standard Strips (Figure 4). We introduced these stylized artifacts in Study 2, with the intention of giving participants physical items to think with [72] when divulging their attitudes towards privacy. In this section, we will

describe these materials and will then explain how they were used in the following subsection, *Participatory Privacy Elicitation Activity Design*.

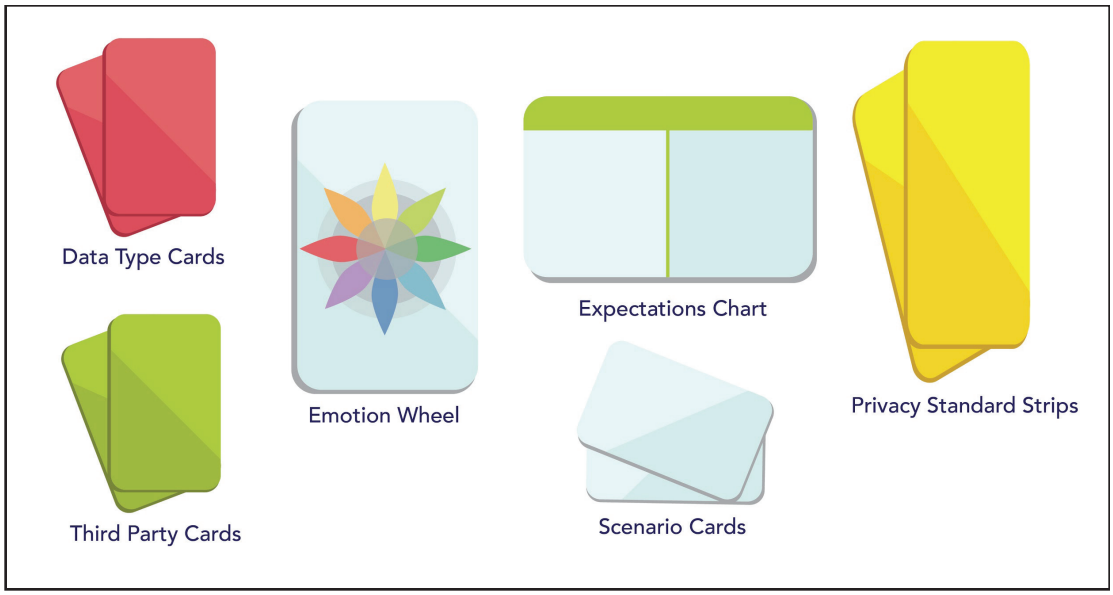


FIGURE 4. Overview of materials developed for Participatory Privacy Elicitation Activity. The materials include red Data Type Cards, green Third Party Cards, the Emotion Wheel, the Expectations Chart, Scenario Cards, and Privacy Standard Strips.

The Scenario Cards each featured a use-case scenario with an adaptive assistive technology. Two Scenario Cards were printed and given to the participant during the corresponding activity. The red Data Type Cards were each labeled with different data types including Contact Data, Credit Card Data, Cookies, Health Data, Search Queries, Typing Data, and Pointing Data. Blank red cards were also printed with this set. The Data Type Cards were used during the *Stage 1 Data Type Activity*. The green Party Cards were each labeled with different third parties including Family, Friends, Doctors and Medical Professionals, Employer, Insurance Company, Government, Private Organization that Built Program, Advertisers, Nobody and Everybody. Blank green cards were also printed with this set. Party Cards were used during the *Stage 1 Expectations Activity* in conjunction with the Expectations Chart. The Expectations Chart is

divided into two columns, with the header of the left column titled, “I expect these parties to have access to my data,” and the header of the right column titled, “I do NOT expect these parties to have access to my data.” The Emotion Wheel is a printed copy of Plutchik’s Wheel of Emotions, which segments the core of the wheel into what Plutchik identified as our eight primary emotions: Anger, Anticipation, Joy, Trust, Fear, Surprise, Sadness, and Disgust. Each of these emotions are segmented into color-coded sectors, with related emotions decreasing in intensity as the emotion label’s distance from the core of the wheel increases. The Wheel of Emotions is used during the *Stage 1 Emotions Activity*. The yellow Privacy Standard Strips are each labeled with 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, and No Rules. The Privacy Standard Strips are used during the *Stage 2 Privacy Standards Activity*.

To view the actual materials used in the Participatory Privacy Elicitation Activity, please refer to Appendix C.

Participatory Privacy Elicitation Activity Design

The primary motivations for creating the participatory privacy elicitation activity were to develop a methodology specifically tailored to extracting perceptions and attitudes pertaining to privacy within a defined subpopulation, and to actively involve our participants in designing privacy standards for adaptive assistive technologies. Brandt stresses the importance of game playing as a positive basis for learning amongst designers and users [12]. Introducing game elements to the study can also increase intrinsic motivation to accurately identify their attitudes

towards privacy and make, what may be perceived as dull, privacy standard discussion more interesting [19]. Although the activities we created are game-like in essence, we classify them as activities rather than games. This classification was made as a strategic effort to discourage participant trivialization of the research study due to gamification[19]. Also, because our participants were older adults, we did not want our participants to feel infantilized [68] by calling the study "a game". The final activity was a result of multiple iterations informed by internal pilot tests amongst our researchers, and further refinement after conducting three external pilot tests with individuals outside of the research group. Figure 5 depicts a high-level overview of the finalized activity format for Study 2.

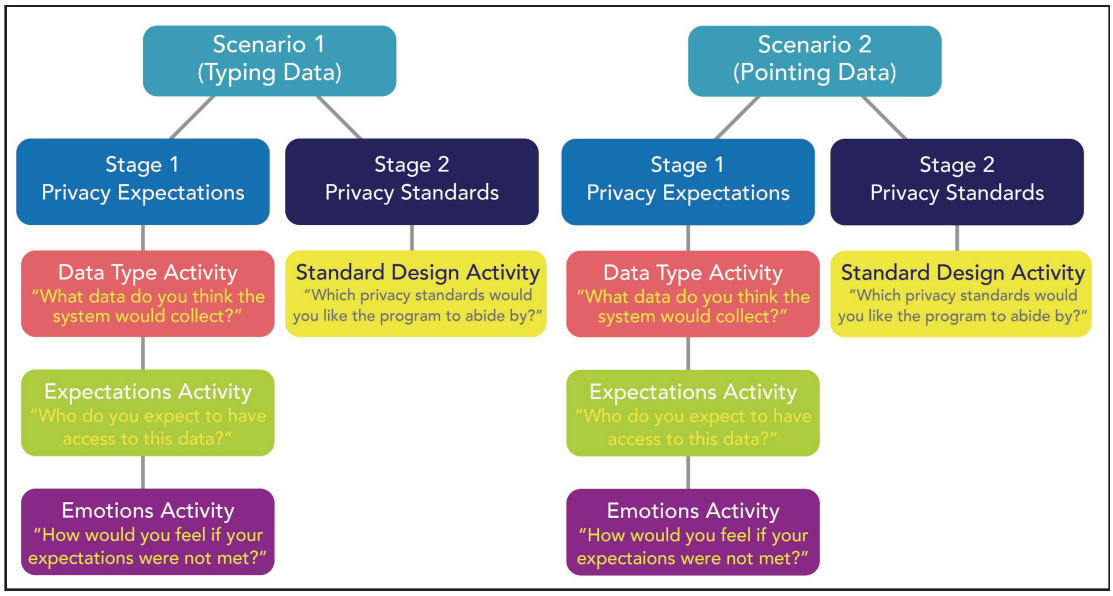


Figure 5. High-level overview of activity format for Study 2 sessions. Two scenarios featuring adaptive assistive technologies were developed. Each scenario consisted of two stages: Stage 1 - Privacy Expectations, and Stage 2 - Privacy Standards. Stage 1 consisted of an interactive activity, privacy expectations activity, and an emotion-based activity. Stage 2 featured a privacy standards design activity where users were prompted to create their ideal privacy rules for how the program should collect data.

We designed two scenarios, both of which featured a different adaptive assistive system. We introduced scenarios to restructure the context of use situations with these technologies, and to

elicit new insight from our participants prompted by these predetermined contexts [83]. All first scenario activities were completed before moving on to the second scenario. The featured scenario text was placed on the table for the participant's reference during corresponding activities.

The first scenario involved a fictitious adaptive assistive Spell Check application, SuperSpeller, that functions by monitoring user typing data. Participants were shown a demo of the popular cloud-based writing assistance application, *Grammarly* [26], to demonstrate SuperSpeller's potential functionality. The second scenario featured our design probe from Study 1, PINATA, an application that adapts to users' changing pointing abilities by collecting user pointing data. Although participants had interacted with PINATA in the previous study, we opted to demo the program again for participants due to the six-month time lapse since the first study, and to provide participants with the opportunity to view the program for a second time rather than having to entirely recall its functionality.

Each scenario consisted of two identical activity stages: Stage 1 - Privacy Expectations, and Stage 2 - Privacy Standards (Figure 4). Stage 1 involved three sub-activities: the *Data Type Activity*, the *Expectations Activity*, and the *Emotions Activity*. Stage 2 featured a *Privacy Standards Design Activity*.

In Stage 1, participants were first asked to discuss what types of data may be collected in the application featured in the given scenario. This portion of Stage 1 is defined as the *Data Type Activity*. The purpose of this activity was to **learn the users' understanding of what data may be collected by adaptive assistive technologies**. After the participants offered their initial response, the researcher placed the red data type cards in front of the participant. These cards

were each labeled with different data types including Contact Data, Credit Card Data, Cookies, Health Data, Search Queries, Typing Data, and Pointing Data. The participant was then asked to walk the researcher through whether they believe any of the data types displayed on the cards would be collected by the application in the given scenario. Blank data type cards were offered to the participant if they wanted to include a new data type.

The next sub-activity in Stage 1 is defined as the *Expectations Activity*. In this activity, participants were asked to discuss their expectations about which parties would have access to their data collected from the application featured in the given scenario. The purpose of this activity was to **learn the users' expectations of who has access to their data collected by adaptive assistive technologies**. To conduct this activity, the researcher placed the Expectations Chart in front of the participant. The Expectations Chart was divided into two columns, with the header of the left column titled, "I expect these parties to have access to my data," and the header of the right column titled, "I do NOT expect these parties to have access to my data." The researcher would then place the green third party cards on the table in front of the participant. These cards are each labeled with different third party types including Family, Friends, Doctors and Medical Professionals, Employer, Insurance Company, Government, Private Organization that Built Program, Advertisers, Nobody and Everybody. The participant was then asked to place the third party cards into the Expectations Chart based whether or not they expected this party to have access to their data collected by the application in the given scenario. The participant was asked to justify their reasoning when placing the third party cards in the chart. Blank third party cards were offered to the participant if they wanted to add a new third party to the chart.

The final sub-activity of Stage 1 is defined as the *Emotions Activity*. In this activity, participants were asked to discuss how they would feel if their expectations, discussed in the previous activity, were not met. The purpose of this activity was to **understand how participants' emotions are entwined with their privacy expectations concerning adaptive assistive technologies.** To conduct this activity, the researcher placed Plutchik's *Wheel of Emotions* in front of the participant. The researcher then instructed the participant to refer to the wheel during the activity when identifying how they would feel in the given scenario. To provide clarity, the researcher gave an example of how she would use the *Wheel of Emotions* to describe how she felt during an event, placing cards down on the different emotions as she named them. The researcher would then refer to the *Expectations Activity* chart, and ask the participant how they would feel if their expectations were not met for each party. Furthermore, if a participant had placed the Advertiser third party card in the *I do NOT expect this party to have access to my data* column in the previous activity, then the researcher would ask the participant to use the *Wheel of Emotions* to identify how they might feel if advertisers *did* have access to their data collected by the application. The participant was then asked to discuss why they might feel this way. This was repeated for each third party card. Once all third party cards had been placed on the *Wheel of Emotions* according to how the participant would feel if their data sharing expectations were not met, the researcher observed the wheel for clusters of third party cards to prompt further questions. For example, if the participant had placed a majority of the third party cards on the *annoyance* portion of the wheel, the researcher might ask the participant if they can think of any provisions with how their data is handled by these parties that would make them feel differently or less annoyed. This would conclude Stage 1.

Stage 2 featured a *Privacy Standards Design Activity*, where participants were asked to design standards to guide how their data is handled by the application in the given scenario. The purpose of this activity is to invoke participatory design to **learn how participants want adaptive assistive technologies to handle their data.** The researcher would begin the activity by placing the yellow privacy standard strips in front of the participant, and reading a brief description of the existing standard. These privacy standard strips included the Health Insurance Portability and Accountability Act (HIPAA), the General Data Protection Regulation (GDPR), Privacy Policy, Terms of Service, and Data Use Agreement. The participant was also given two additional privacy standard strips that had not been generated from existing standards: My Custom Rules (giving participants the opportunity to make their own standards), and No Rules (giving participants the opportunity to forgo any rules or standards with the handling of their data). The participant was then asked which of these standards they would like to guide how the application in the scenario handles their data. They were told they could select as few or as many standards as they would like. The participant was then asked to explain why each standard was either selected or unselected. Next, the researcher bought the expectations chart from Stage 1 back into focus, and asks the participant how they would like their selected standards to guide how their data is handled with the third parties. The participants were then asked to use the Emotion Wheel to describe how they would feel if their chosen standards were implemented by the application.

Participant Recruitment

We contacted our participants from Study 1 and asked if they would be interested in participating in a follow-up study. Six of the eight participants from Study 1 agreed to partake in the second study (Table 2). We chose to recruit our former participants with interest in how the lapse in time and pronounced difference in methodologies between both studies would shape the data. All participant interviews took place during the month of September 2018, and were conducted in Howard County public libraries.

ID	Former ID	Age	Gender	Career History	Reason for Pointing Difficulty	Weekly Internet Use (Hours)	Perceived Value of Internet
P1	P2	82	Male	Forestry	Essential Tremors	25-30 Hours	Somewhat Valuable
P2	P4	87	Male	Air Force Pilot, Computer Specialist, Accountant	Essential Tremors	8-9 Hours	Very Valuable
P3	P7	73	Male	Educator (University)	Essential Tremors	14-28 Hours	Very Valuable
P4	P1	71	Female	Customer Service	Essential Tremors	2 Hours	Somewhat Valuable
P5	P3	69	Male	Customer Service	Essential Tremors	30+ Hours	Very Valuable
P6	P5	64	Female	Computer Systems Analyst, Stay-at-Home Mom, Fitness Tech	Essential Tremors	12-14 Hours	Very Valuable

Table 2. A table summarizing the backgrounds of participants from Study 2. Participants were given alphanumeric IDs based on the chronological order in which they participated in Study 2 (i.e P1 represents the first participant, while the last participant is labeled P6). All participants from Study 2 had participated in Study 1. Each participant's former ID from Study 1 is listed in the second column. The participants' age, gender, career history, reason for pointing difficulty, reported weekly internet use in hours, and perceived value of internet access are included in the table. All participants considered themselves retired with the exception of P4, who described being employed part-time.

Limitations

We first deployed the Participatory Privacy Elicitation Activity as a methodology in our second study. As this was the first time the methodology was used in a research study, the novelty of the methodology may be limiting. Limitations in generalization should also be taken into account for our small sample size of six individuals. The data is by no means generalizable to all older adults experiencing variable pointing difficulties [77]. Additionally, our interviews focused on theoretical attitudes about privacy threats when interacting with adaptive assistive technologies, as the participants were given scenarios rather than actually having interacted with the systems. For example, participants were asked *how they would feel* in a particular scenario, or *who they would be comfortable with* having access to their pointing data, rather than the participants actually having experienced the scenarios and reporting their perspectives. Furthermore, we believe participants' responses to be limited to their brief interaction with the scenario description and adaptive assistive technology demos, and could evolve with the participants' actual participation in these scenarios, and/or use of the featured adaptive assistive systems.

Data Analysis

During the study, we captured photographs of the participants' completed activity boards. We also audio recorded and transcribed each interview. Based on the study photographs and transcriptions, the data from each activity was depicted onto ten visualization boards for each participant, totaling 60 visualization boards. Each set of visualization boards included a board displaying participant data from Scenario 1 *Data Type Activity*, Scenario 1 *Expectations Activity*,

Scenario 1 *Emotions Activity*, Scenario 1 *Privacy Standards Design Activity,* Scenario 2 *Data Type Activity*, Scenario 2 *Expectations Activity*, Scenario 2 *Emotions Activity*, Scenario 2 *Privacy Standards Design Activity*, Study 1 Expectations, and Study 2 Expectations. These boards were used as communication artifacts amongst our research team, and tools for identifying high-level themes amongst our participants, and comparing and contrasting their responses. To further distill the data, we conducted an iterative thematic analysis to identify and synthesize themes [11] within the transcriptions. Kellie Gable transcribed the interviews, introducing an initial stage of coding. This included noting keywords, prominent emerging themes, supporting anecdotes, and patterns in the margins of the transcripts. Dr. Foad Hamid, Dr. Amy Hurst, and Dr. Aaron Massey then added a second layer of coding which consisted of further analysis and theme identification. Once the second coding phase had been completed, we then met in-person and discussed the data in extent, further refining our theme classification as a research team.

Figure 6. Thumbnails of ten visualization boards created for P5. Visualization boards depicted from left to right, top to bottom: Scenario 1 *Data Type Activity*, Scenario 1 *Expectations Activity*, Scenario 1 *Emotions Activity*, Scenario 1 *Privacy Standards Design Activity,* Scenario 2 *Data Type Activity*, Scenario 2 *Expectations Activity*, Scenario 2 *Emotions Activity*, Scenario 2 *Privacy Standards Design Activity*, Study 1 Expectations, and Study 2 Expectations.

5: Findings

We defined and thematically grouped our findings after conducting *Study 1: Exploring Attitudes Towards Privacy with Interviews and a Design Probe* and *Study 2: Participatory Privacy Elicitation Activity*. This chapter is broken down into two main sections, where we divulge our findings from each study: *Study 1 Findings* and *Study 2 Findings*. In both subsections, we present our study-specific findings related to our primary *Research Question #1: What are older adults' perspectives, attitudes, and concerns towards privacy in the context of adaptive assistive technologies?* In *Study 2 Findings*, we also present findings related to *Research Question #3: How can researchers use participatory methodologies to elicit privacy attitudes from end-users?* Overall, our findings reveal that participants are motivated to use adaptive assistive technologies, but hold fervent preferences about how their data collected by adaptive assistive technologies should be accessed. Below, we provide a high-level summary of findings from both studies:

Study 1

- Participants conveyed specific privacy concerns related to downloading new software, but valued these programs and would continue to use them.
- Participants experienced computer accessibility barriers because of pointing difficulties, and were motivated to use AATs to overcome these barriers.
- Participants expressed specific concerns about their online privacy, and privacy when using AATs. Most participants were concerned about their data being used and shared without their consent

- Participants felt a lack of agency in controlling their personal data when using online AATs.
- Participants were enthusiastic about using PINATA. They valued system accuracy and were more concerned about false positives than false negatives.
- Participants wanted access to their own collected data to reflect on their own performance.
- Participants were comfortable with their data being collected to improve AATs
- Most participants were comfortable with application developers, medical doctors, and family members accessing their pointing data. They were hesitant about sharing their pointing data with employers, insurance companies, or governments.
- When giving permission to use their data, participants wanted to know how and under what premise it was used.
- Most participants were comfortable with their data being used for medical research or to improve system accuracy, but not for screening or other unknown purposes.

Study 2

- Participants generally expected the assistive typing application to be more expansive with data collection than the assistive pointing application.
- Most participants did not initially identify health data as information that would be collected by AATs. However, they often shifted perspectives on this matter throughout the interview.

- Participants were more open to sharing their collected pointing data with medical professionals and the private organization that built the program, compared to sharing their typing data with these parties.
- Compared to Study 1, all participants experienced changes in their pointing data sharing preferences.
- Participants generally identified more intense emotions when discussing unmet expectations with their typing data compared to their pointing data.
- All participants chose at least two privacy standards to guide how their data is handled in AATs. Participants expressed polarized views with the HIPAA standard, and some felt that the GDPR could give them agency over their data.
- Participants found the activities thought-provoking, and enjoyed the tactile aspect of the activities. They used the materials in creative ways
- Participants cited difficulty with Plutchik's Wheel of Emotions.

Study 1 Findings

Staying Connected: Benefits and Challenges of Using Digital Systems

Participants described many motivations to use computers, access the Internet, and the accessibility issues they experienced due to pointing challenges. Most of the described computer use involved an Internet connection, making it difficult to distinguish between general computer use and Internet access. This feature might be due to the increasingly connected nature personal computing, especially in the context of the study (urban United States).

Benefits of Accessing Computers and the Internet

All participants stated that they regularly use computers and all but one participant (P1) regularly use the Internet (with usage time ranging from 2 hours to 30+ hours per week). Six participants described access to the Internet as "very valuable" and two described it as "valuable".

Participants considered multiple factors when deciding to trust applications. These included recommendations from friends and family (P1, P7), consistent application functionality (P2, P5), positive user reviews (P7), association with a trustworthy company or platform (P3), and software aesthetics (P7). However, all participants (except P1) described concerns about downloading and installing new software. These concerns included their computers being hacked (P4), data leaking through social media (P3), malicious software being installed on their computers (P2, P3) and their identity being stolen (P7). Despite these concerns, all participants valued downloaded applications and would continue to use them.

Cost of Computer and Internet Inaccessibility

Experiencing pointing difficulties had caused computer accessibility issues for most of the participants (all except P6). P1 related how her employment had been affected when she started experiencing pointing difficulties that ultimately forced her to leave her job:

> *"I could not hold that mouse steady enough to be able to do that, and I was like all over the screen… and so my boss said to me, 'Well that's what I hired you for, and that's what I need you for'… Well, I couldn't do it." -P1*

P5 was concerned that emerging interfaces, such as touch screens, might create new accessibility barriers for her when accessing the Internet or driving a car. She was concerned about insurance companies knowing about her tremors because they might "*extrapolate it and say, 'she's going to hit the wrong button [when driving a car]' … since there's so many more … dashboard touchscreen and things, 'she's more likely to have an accident'*."

Given these accessibility challenges, all participants were enthusiastic about research and development efforts to design systems that can monitor their activity and support their specific needs. We will present these views later when discussing participants' input on PINATA.

Privacy Tradeoffs of Using Online Adaptive Systems

Previous Experiences with Online Adaptive Systems

All participants used adaptive websites and services. These included e-commerce websites such as Amazon.com and BestBuy.com that suggest products from previous purchases (P1, P2, P3, P4, P5, P7), search engines such as Google that present search results from previous searches (P2, P5, P6, P7, P8) and gaming websites that suggest new games based on played games (P3). No participant described using an adaptive system for accessibility.

Privacy Concerns when Using Online Adaptive Systems

Every participant except P1 had concerns about online privacy. These concerns included a general fear that "everybody is watching me" (P2) and the global scope of the Internet (P6), concerns about hacking (P4), data mining and malware (P5), and identity theft (P7). We observed that participants (P3, P4, P5) with computing work experience expressed more specific concerns

(e.g., data mining and targeted advertising), than participants (P1, P2, P6, P7) without this work experience. The following quotes from P5 and P7 highlight this difference:

> *"They would want to try to find out political leanings or what your voting record might be… and sometimes, it can be on a lower level or more personal level, 'Oh, they've booked a cruise for August. There's not going to be anybody in that house for two weeks.'"–P5 (specific concern)*

> *"I've gotten to the point where I believe I'm being tracked in one way or another by anything I use." – P7 (general concern)*

Several participants (P2, P5) made references to current news stories about data breaches that had happened on popular platforms, such as Facebook [80].

What Data is Collected, and How is it Used?

When asked about what type of data online applications were gathering, several of the participants described it as "everything", including "keystrokes" (P5), "time spent on screens" (P7), "whatever they can get" (P4, P6) and even "what individuals are thinking and feeling" (P6). Some participants were more specific and identified purchasing habits and search results as the type of data usually collected (P1, P2, P3, P7, P8).

When asked how their data could be used, participants described scenarios informed by their previous job experiences. Three participants (P3, P4, P5) had worked as computer specialists or analysts. They valued the integrity of the system itself and correlated improved privacy with

higher system quality. For example, P3 discussed their experience working at nonprofit to justify data collection:

> *"We collected data. We had a search you could find childcare online-- who was looking, where they do the most looking … We'd make up a monthly report, and I was told we'd have to do this because the main funding was a state grant. … So, I mean there is reason for gathering data beyond selling it." –P3*

Participants had many concerns about how their data could be abused. They expressed concern around their data being shared for profit and for marketing purposes (P2, P3, P5, P6, P7, P8), for identity and property theft (P1, P4), for influencing political leanings (P5), and for online behavior manipulation (P7). Most of these concerns reflected how data could be used without explicit consent. Even when participants were comfortable with a specific trusted website or application using their data, they were not comfortable with it being shared with others.

> *"They [Amazon website collecting data] are okay … what bothers me is when they sell it to other sites." –P3*

How can I Control my Data? The Real Cost of Using a System

When asked about their level of control over their personal data when using online adaptive systems, most participants (P2, P4, P5, P6) described feeling a lack of agency on their part. When asked how he would like the software to assure him that his data is being used as promised, P4 answered, "I don't know that they can prove anything." P5 echoed P4's sentiments: "Without having something to calibrate against, you could tell me anything you wanted."

For some participants (P3, P6) this feeling of helplessness was somewhat mitigated if they paid for the application.

> *"I'd have to admit that if I paid for it, and they swear they're not going to do something ... then I can beat on them for a justification at least. I've never had to do that, but at least it does make me feel like if I paid, by God, you're going to hear about it if I don't like it." –P3*

Another participant described how he felt a lack of control over his data once it was collected, comparing giving up data to paying for something with cash:

> *"If you give them your permission it's pretty much like giving them money; I can't complain how you spend that." –P2*

Another participant described how not paying for a service made her wonder what hidden costs she way paying:

> *"I don't trust them when it's free because I think any time it's free, then there's a clause behind it … When things are free, what are the obligations?" -P6*

These comments show that participants are generally aware that their data might be collected and used in ways that they might not approve of. This awareness is combined with a perceived lack of choice in how they can control their data when using online systems. These comments underline the loss of control over personal data with "free" services.

Privacy Tradeoffs of Adaptive Assistive Technologies

The following findings emerged when participants interacted with PINATA, as an example of an adaptive assistive technology to help with pointing challenges.

Increasing Accessibility with Automatic Assistance

All participants (except P4) were enthusiastic about using PINATA and would recommend such assistive software to friends. P4 explained that most of the difficulties he experienced were with

using a keyboard and did not feel PINATA would be useful for him. All participants were comfortable with their data being collected to improve system usability and accuracy. They liked how their data could be monitored to automatically adapt the bubble cursor's shape and selection area. All participants (except P8), preferred automatic mode rather than manually changing the cursor. P3 asked about how installing PINATA might impact his wife's computer use and if it could distinguish between the two of them.

Accuracy of Adaptive Assistive Technology

Participants valued system accuracy highly and described how recognition errors can negatively impact them. When asked about what type of recognition errors they were most concerned about, participants had more negative feelings if the system recognized errors that were not there (i.e., *false positives*), than if it failed to recognize errors that were present (i.e., *false negatives*). When considering what they would do about a system with high false negatives, only one participant (P3) said he would uninstall it. In the case of false positives, negative reactions were more severe: P1 stated that she would visit her neurologist, P7 and P5 stated they would feel "frustrated", and P2 and P6 stated they would want feedback and would not know otherwise. These results are consistent with previous research on users' asymmetric attitudes towards errors in automatic recognition systems [6]. Several participants (P2, P4, P5) were comfortable with their user data being collected to improve system accuracy and overall functionality.

Keeping Users Informed About Their Collected Data

All participants found the sample data visualizations interesting and potentially helpful in understanding their ability (Figure 2). Several participants wanted more information in the

visualizations (P2, P3, P5). P2 wanted the errors to be mapped to different times of the day. P3 and P5 wanted to have the exact rate of errors or percentages of total errors that had occurred for each website. P7 said it would help him distinguish between his pointing difficulties. P1 stated that she would probably look at the visualizations but was unsure if she was going to change her behavior based on them.

While the participants wanted to access their data through visualizations, they were not enthusiastic about changing the data (e.g., to correct system errors). Only three participants (P1, P5, P8) wanted to be able to delete their data. Five participants (P2, P4, P5, P6 and P7) did not want to edit the data and were concerned about data integrity if this was possible. Four participants (P2, P4, P6 and P7) believed changing or editing the data would impact the accuracy and reliability of the system.

"It's not data then. If you can manipulate it, it's basically useless. "–P2

Who Should Have Access to my Pointing Data?

	Yes		Maybe		No	
Private (P) Anonymized (A)	**P**	**A**	**P**	**A**	**P**	**A**
Family	6	7	1	0	1	1
Private Organization that Built Program	5	7	2	1	1	0
Doctors and Medical Professionals	6	8	1	0	1	0
Employer	1	3	1	1	6	4
Government	1	4	1	0	6	4
Insurance Companies	0	1	1	0	7	7

Table 3. A table summarizing data from participants regarding their willingness to share Private (P) or anonymized (A) data with different organizations. Participants were most comfortable sharing data with family members, medical professionals, and private assistive software companies.

While participants saw the value in collecting this data, some had concern about what would happen to this data over time and who would have access to it (Table 3). All participants except P4 were comfortable giving their family and medical doctors access their data. However, P1 and P7 wanted to control who could view their data and know why they wanted to see it.

In contrast, P8 was the only participant comfortable with their employer seeing their data. She justified this sentiment on the basis that she would not work for someone she didn't find trustworthy. Only 3 participants (P3, P5 and P7) would share data with employer if it was anonymized. P7 mentioned that the collected data "should be considered as medical information"

and its privacy protected similarly. Other participants described concern that their employers might misjudge their abilities if they could access this data:

> *"You wonder okay are they going to be able to tell if I have medication that helps with it ... Would it affect a hiring decision?" – P5*

> *"I would feel that my employer would feel that I wasn't competent." -P6*

Participants were generally hesitant to share data with insurance companies or government organizations, and a few expressed exceptions. P3 would consider sharing his data with an insurance company if they asked permission first. Our participants were evenly split on sharing their data with the government. P2 stated that it would depend on how the data is used: he was OK sharing his data if it was used for medical research but not if it was used for intelligence or military applications. Half of the participants (P2, P3, P4, P5) were comfortable if their data was shared anonymously with the government for research purposes.

> *"They don't really need to hold that data—I mean I'll give it to researchers anonymously ... I read The Life and Times of Henrietta Lacks [an African-American woman whose cells were used for research]." – P5*

Finally, all participants were comfortable sharing their anonymous data with the company that developed PINATA. However, P6 stated that she wanted to know why her data was needed before she would agree for it to be used. Only one participant (P5) wanted their data to be anonymized when shared with the developer company and two participants (P4, P6) wanted to know how their non-anonymized data was going to be used if shared.

Study 2 Findings

Expectations of Data Collection for Adaptive Assistive Technologies

The following findings emerged when participants were given two scenarios, respectively featuring a spelling and pointing adaptive assistive technology. Participants were asked what types of data they expected would be collected by these systems.

Data Collection: Assistive Typing Program

In the first scenario featuring an adaptive assistive spelling and grammar application, all participants expected the program to collect their typing data (P1, P2, P3, P4, P5, P6). Participants offered varying interpretations of typing data. All participants believed the program would collect spelling and grammar errors (P1,P2, P3, P4, P5, P6). Some participants believed the program would learn the user's speech patterns (P1), track the rate at which one types or how often one hesitates to type (P3), collect the content of what is typed (P1, P2, P5), track keys that are held down too long (P6), and note repeated typing errors of the same nature (P6).

After being asked what types of data the participants expected would be collected, they were shown a set of data type cards and asked if they expected any of the displayed data types to also be collected by the spelling application. With the exception of P2, all participants identified one or more of the cards as a data type that would be collected by the spelling application. P2 rejected the idea of any data types, other than typing, being collected by the system, pointing to the cards and justifying:

> *"See, a lot of these would [be collected by] Google or something else." - P2*

P2 demonstrated a mental model of a locally-bound word processing application, that collects the minimal data needed to function, contrasting in nature from his provided example of "Google". The remainder of the participants identified pointing data (P1, P4, P5, P6, P3-*Maybe*), contact data (P1, P3, P4, P6-*Maybe*), search queries (P1, P3, P5, P4-*Maybe*), and Cookies (P3, P5, P1-*Maybe*) as data types that they would expect the spelling application to collect. Most participants, with the exception of P5, **did not** expect the application to collect their credit card data.

Data Collection: Assistive Pointing Program

In the first scenario featuring an adaptive assistive pointing application, all participants expected the program to collect their pointing data (P1, P2, P3, P4, P5, P6). Participants offered varying interpretations of pointing data, expecting the system to collect the severity of their shaking (P1, P3), pointing performance based on the time of day (P1), target clicking patterns (P2, P4), the degree of overshooting or undershooting the target (P3), and general pointing performance (P1,P3,P5, P6).

After revealing their initial expectations of collected data types, they were shown a set of data type cards and asked if they expected any of the displayed data types to also be collected by the pointing application. In contrast to Scenario 1 featuring the assistive spelling application, participants did not expect the assistive typing application to be as expansive with data collection. The mental model of assistive pointing applications collecting less data is illustrated through P5's commentary in Scenario 2. With the assistive typing application, he had selected all

data types but only expected the assistive pointing application to collect pointing data, explaining:

> *"It shouldn't [collect these data types]. It's not actually reading what you're pointing on, just if you're actually hitting it." -P5*

None of the participants expected the assistive pointing application to collect contact data, credit card data, search queries, or cookies, and only two of the participants (P1,P6) expected the system to collect typing data.

Perceptions: Do Adaptive Assistive Technologies Collect Health Data?

Besides one participant (P5) in Scenario 1, participants did not initially identify health data as a data type that would definitively be collected by adaptive assistive technologies from either scenario. However, all participants wavered on their initial inclination throughout the activities, often shifting perspectives, citing that the systems wouldn't explicitly collect health data, but that health conditions could be identified through collected data. P4 illustrates this conflicting phenomenon, initially stating that PINATA would not collect users' health data, but later expressing that she wanted doctors and medical professionals to have access to her collected data to indicate the state of her health condition.

> *"If my Essential Tremors 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*

P4 views PINATA as a system capable of revealing the severity of her health condition to medical professionals, but had not explicitly identified these systems as collecting "health data".

This tension is further illustrated by our session with P1, as he had believed PINATA could be capable of capturing the degree to which the user was shaking, but soon after expressed:

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

Some of our participants (P2 and P6) were adamant that the adaptive assistive technologies from both scenarios **should not** collect health data. In our session with P2, he initially dismissed the premise of the first scenario's adaptive assistive technology collecting health data. He stressed that adaptive assistive technologies, *"should not have access to [your] medical information, unless you want them to."* Later in the interview, he shifted his perspective on this matter, referencing the linking of health conditions to collected typing data or search queries:

> *"It could [collect health data]... say you're on the internet and you're googling some health thing-- Somebody could say, 'Oh, they're asking that!? He's got that, that, and that!" -P2*

In our session with P6, she claimed that health data should not be collected by adaptive assistive technologies, but understood that this does not necessarily mean data of this nature cannot be obtained by these systems:

> *"They shouldn't, but does it [collect health data]? It might not appear as health data to you or me, but I'm guessing that if it's there, there will be someone that could say this is characteristic of someone with this kind of neurological thing." -P6*

P3 echoed this sentiment, hesitant to explicitly identify "health data" as a data type collected by adaptive assistive technologies, but suggested that health data could be indirectly collected:

> *"Some of the qualities of typing may be indicative of the Essential Tremor if it's sensitive somehow to.. multiple hits on a given key.. It's not a direct assessment of [a health condition], but it might be correlated." -P3*

Expectations of Who Should Have Access to My Data Collected From Adaptive Assistive Technologies

We asked participants who they expected to have access to their data collected in both scenarios, featuring a typing and pointing based adaptive assistive technology. First, we analyzed their responses for each scenario.

Assistive Typing Program - Who Should Have Access to My Typing Data?

	P1	P2	P3	P4	P5	P6	Yes Total	Maybe Total	No Total
Family	No	No	No	No	No	No	0	0	6
Friends	No	No	No	No	No	No	0	0	6
Private Organization that Built Program	Yes	No	Yes	No	No	Maybe	2	1	3
Doctors and Medical Professionals	No	No	Maybe	No	No	Maybe	0	2	4
Employer	No	No	No	No	No	Maybe	0	1	5
Government	No	No	Maybe	No	No	No	0	1	5
Advertisers	No	No	Yes	No	No	No	1	0	5
Insurance Companies	No	No	Yes	No	No	No	1	0	5

Table 4. A table summarizing data from participants regarding their expectations of who should have access to their data collected from an assistive spelling application. The columns represent the individual participant responses regarding whether or not they expect a party to have access to their data. The rows indicate the third party in question. The last three columns summarize the response totals regarding how many participants expect, might expect, or do not expect parties to access their collected data. Half of the participants did not want any third parties to have access to their data. No participants wanted family or friends to access their typing data, and most participants did not want employers, government, advertisers, or insurance companies to have access to their tying data.

In the first scenario featuring an adaptive assistive typing application, half of the participants were adamant that nobody should have access to their typing data (Table 4) [P2, P4, P5]. Some participants explained their blanket preferences to be rooted in third parties' lack of justifiable reason for access and simply not being privy to their data:

> *"I don't think there's a reason for them [to have access to my data] because either I don't want them to, or they don't have any business!"-P2*

> *"None of those [parties] need to know any of that [pointing to data type cards]." -P5*

P4 presented her value in personal privacy as justification for her preference for no parties having access to her collected data:

> *"I'm a private person, and I don't want just anybody going and looking at [my data]." - P4*

P1 and P3 expected the private organization that built the program to have access to their personal data collected from the assistive spelling application. They indicated that their use of the data to maintain the application was justified. P6 echoed this sentiment, explaining that she might be comfortable with the private organization accessing her data under the conditions that they obtain her consent and use the data only for program improvement. Although P1 was willing to share his data, he stressed his strong preference for the private organization that built the program to maintain 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*

All participants, with the exception of P6, did not expect employers to have access to their typing data. Participants cited lack of trust [P1], lack of entitlement to the collected data [P2], and fear of the data leading to negative repercussions in their employment [P1, P6]. P6 described a scenario in which an employer's access to her typing data could lead to an unfair judgment of her productivity:

> *"Would there be any potential of, 'Look at this lady! She goes backwards as much as she goes forward-- She's not very efficient!'?" - P6*

Despite her apprehension with employers accessing typing data from assistive applications, P6 stated that she would feel comfortable if first asked for her consent:

> *"If I were employed, I could accept that they'd want to see what I'm doing… it would be upon my invitation that I share it." - P6*

All participants, with the exception of P3, did not expect insurance companies, advertisers, or government to have access to their typing data. Participants did not want their typing data shared with insurance companies because they believed it would be used to enhance their bottom line [P1], or that it could lead to false positives with an incorrect diagnosis of a health condition:

> *"I think [insurance companies are] going to use [my performance data] to enhance their bottom line."-P1*

> *"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 alluded to fatigue and annoyance from perceived over-saturation of digital advertising, and did not want advertisers to have access to their typing data:

> *"They don't do you harm, but why have them? They're just a nuisance!" -P2*

"I get too many popups, too many advertisements, too many emails trying to get me to buy something." -P4

Most participants expressed that they did not want government to access their typing data, sometimes referring to specific departmental agencies:

"I don't think the government has any place in my personal life… [but] every once in a while, I get on the phone and I say, 'Okay, NSA (National Security Agency)-- Listen Carefully!" -P1

"I don't think I'd like the government looking into it, like the IRS (Internal Revenue Service)" -P4

"I wouldn't type [if the government had access to my typing data]. I'd find another method." -P2

P3 explained that he would be comfortable with the government having access to his typing data, in a scenario in which,*"there would be some kind of subpoena, warrant, or probable cause."*

None of the participants expected their friends or families to have access to their typing data collected by the application, citing personal privacy, and lack of reason for access:

"I'm just very private… I think maybe younger people aren't as private as us old people… because they're on Facebook and they just expose everything about themselves." -P1

"I don't see a reason, at least immediately, where friends or family should have that information." -P3

"Friends-- They don't need [my typing data]. Family-- I might want to be the one to present it to them." -P6

Assistive Pointing Program - Who Should Have Access to My Pointing Data?

	P1	P2	P3	P4	P5	P6	Yes Total	Maybe Total	No Total
Family	No	Yes	No	No	No	No	1	0	5
Friends	No	No	No	No	No	No	0	0	6
Private Organization that Built Program	Yes	Maybe	Yes	No	Yes	Maybe	3	2	1
Doctors and Medical Professionals	Yes	No	Yes	Yes	No	Maybe	3	1	2
Employer	No	No	No	No	No	Maybe	0	1	5
Government	No	No	Yes	No	No	No	1	0	5
Advertisers	No	No	Yes	No	No	No	1	0	5
Insurance Companies	No	No	No	No	No	No	0	0	6

Table 5. A table summarizing data from participants regarding their expectations of who should have access to their data collected from an assistive pointing application. The columns represent the individual participant responses regarding whether or not they expect a party to have access to their data. The rows indicate the third party in question. The last three columns summarize the response totals regarding how many participants expect, might expect, or do not expect parties to access their collected data. Half of the participants were comfortable with the private organization that built the program and doctors and advertisers accessing their pointing data. No participants were comfortable with their pointing data being accessed by insurance companies or friends.

In the second scenario featuring an adaptive assistive typing application, participants discussed their expectations of who should have access to their collected data. Half of the participants expected the private organization that built the program (P1, P3, P5) and doctors and medical professionals (P1, P3, P4) to have access to their collected pointing data. Our participants cited the private organization that built the program's need for data access to update the program (P1, P3, P5, P6) as justification for approved access.

"I'd be okay with [the private organization that built the program] using my data to finetune [the program]. How else are they going to get the feedback?" -P6

"If [the private organization that built the program] wants to know how to improve the program, that's alright." -P2

Participants (P1, P3, P4) were enthusiastic about voluntarily sharing their pointing data with their personal doctors and medical professionals, viewing their pointing data as a valuable means to providing more 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

No participants, with the exception of P3, were comfortable with the government or advertisers having access to their pointing data. Participants discussed the government's lack of need or right to access their pointing data:

"I don't think the government needs to be involved." - P1

"What right do they have?! I'm just an elderly woman… why would [the government] be interested in [my pointing data]? -P4

P3 provided an alternative view, that government access to aggregate pointing data, collected from an assistive pointing application, could potentially benefit him:

"To the degree that PINATA would provide information to the regard of a disability or degree of impairment, I could think of government agencies of whom that would be useful for me at the aggregate level." -P3

Most participants did not want advertisers to have access to their pointing data, because of perceived lack of need, but did not view them as particularly threatening:

> *"I don't think they need it. 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*

> *"I can't think of any reason for them to access my pointing data." -P2*

Five of the participants did not want employers to have access to their pointing data (P1, P2, P3, P4, P5), and one participant (P6) might want employers to access her pointing data. Participants mostly discussed scenarios where access to their pointing data could result in harmful consequences at work:

> *"I think the pointing data would point them in a direction-- I think they would wonder, and when they start to wonder, then they figure out how to get the information, or they don't talk to you directly… 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 provided an alternative perspective, suggesting that consensual access to her pointing data could assist in the process of identifying what accommodations she may need in the workplace:

> *"An employer may need to know what accommodations I need, and this might be a diagnostic tool to support data from a diagnosis from the medical profession." -P6*

None of the participants expected insurance companies or friends to access their pointing data. Participants offered scenarios where insurance companies could use their pointing data to make unjustified data extrapolations (P1), increase rates (P1), fuel insurance bias (P3), and unreliably conclude a health condition (P6):

> *"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*

"We've heard of bias in insurance rates, for example with regard to zip codes, and I've got no way of restricting that information. So, here [with my pointing data], I'd feel uncomfortable with [sharing] that." -P3

"They really don't need [my pointing data]. They don't need it from this application. I want them to get it from a neurologist, not from a generalized tool." -P6

Participants mainly cited protection of their general privacy regarding their preferences for restricting friends' access to their pointing data. One participant discussed a more specific privacy concern, proposing that access of this nature could lead to harmful interpersonal consequences:

"I can see someone saying, 'I'm not going to marry you because I don't want my kid shaking.' I think for family, it should be shared. But for potential family, it should be a voluntary sharing of information by two individuals." -P1 (Specific Privacy Concern)

"These are sort of basic privacy issues. If I want to point to a site that has pretty women, I don't necessarily want that all over." -P3 (General Privacy Concern)

Study 1 Versus Study 2 - Who Should Have Access to My Pointing Data?

We asked participants who they expected to have access to their pointing data in both studies. We compared participant responses from Study 2 with their previously expressed data sharing expectations, revealed six months prior in Study 1.

	P1		P2		P3		P4		P5		P6	
Study 1 (S1) Study 2 (S2)	**S1**	**S2**	**S1**	**S2**	**S1**	**S2**	**S1**	**S2**	**S1**	**S2**	**S1**	**S2**
Family	Y	N	N	Y	Y	N	M	N	Y	N	Y	N
Private Organization that Built Program	Y	Y	M	M	Y	Y	Y	N	Y	Y	N	M
Doctors and Medical Professionals	Y	Y	N	N	M	Y	Y	Y	Y	N	Y	M
Employer	M	N	N	N	N	N	N	N	N	N	N	M
Government	M	N	Y	N	N	Y	N	N	N	N	N	N
Insurance Companies	N	N	N	N	N	N	N	N	M	N	N	N

Table 6. A table summarizing data from Study 1 and Study 2, where participants revealed their expectations of who should have access to their data collected from an assistive pointing application. The columns represent the individual participant responses for Study 1 and Study 2: Y=Yes, M=Maybe, N=No. The rows indicate the third party in question. Red cells indicate a more restrictive shift in privacy preferences for that party, while green cells indicate a less restrictive shift in privacy preferences. Privacy preference shifts occurred most frequently regarding data sharing with family members.

In Studies 1 and 2, we asked participants who they were comfortable with having access to their non-anonymous pointing data. We compared participants' pointing data sharing preferences with their previously revealed preferences from Study 1 (Table 6), conducted six months prior. We observed shifts in pointing data sharing preference amongst all six of our participants who returned for the second study. Overall, we observed 19 instances where there was no change in pointing privacy preference, 12 instances where participants preferred more restrictive access to their pointing data, and five instances where participants preferred less restrictive access to their pointing data. Half of our participants only exhibited more restrictive changes in their data sharing preferences (P1, P4, P5), while the other half of participants exhibited instances of both more restrictive and less restrictive data sharing preferences amongst third parties (P2, P3, P6).

We observed sharing preference shifts amongst all third parties discussed in the studies. The greatest number of shifts was observed in sharing preferences with family members, as all participants changed their original responses shared in Study 1. All of the participants (P1, P3, P4, P5, P6), with the exception of P2, favored more restrictive access for family members compared to Study 1. Participants explained that they wanted to have discretion in which family members could access their pointing data, and one participant cited her recent experiences with certain family members as reason for favoring more restrictive access:

> *"It could be my recent dealings with my siblings. I'd be okay with my children and my spouse [accessing my pointing data] but when we get to siblings-- I don't necessarily want to share all the details of a health concern or performance." -P6*

No discernible pattern was detected in the remainder of sharing preference shifts amongst third parties. Participants opting for more stringent data sharing preferences justified their changes with references to privacy-related news stories (P5), changes in personal life (P6), and continued thought and discussion about privacy (P4, P6). P5 reflected on his previous responses in surprise, offering that his changed preference for more restrictive sharing may be due to the influx of privacy-related news stories involving large technology companies:

> *"It's hard to imagine I said that [I might be comfortable with insurance companies accessing my pointing data]. I can see why they would be interested in it, but I'm certainly not comfortable with it… Maybe I've been bombarded since then with so much, you know, 'Google is ruining your life' kind of thing." -P5*

Exploring Emotions: What if My Data Sharing Expectations Were Not Met?

In Study 2, participants were asked to discuss how they might feel if their data sharing expectations, for both assistive typing and assistive pointing applications, were not met. We

asked participants how they might feel if third parties, discussed in the data sharing expectations activity, had access to their data. Participants were asked to identify emotions they might experience in these scenarios, to give our research team a better understanding of how people may feel if their privacy expectations are not met when using adaptive assistive technologies. Overall, identified emotional responses amongst participants were quite varied in both scenarios. Participants expressed they would feel annoyance (P1, P2, P3, P5, P6), anger (P3, P5, P6), disgust (P2, P4), surprise (P3, P6), acceptance (P1, P6), trust (P3), violation (P4), apprehension (P1), disapproval (P3), anticipation (P4), and fear and terror (P1) if their typing data sharing preferences were not met. Annoyance was projected most often by participants (17 instances), followed by anger (10 instances) and disgust (8 instances). The emotions identified by the participants across each third party were varied, although some third parties elicited more intense emotional responses based on Plutchik's emotion wheel. Participants exhibited the most intense emotional response to 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).

Compared to the first scenario, participants identified less intense emotions when discussing how they would feel if their pointing data sharing expectations were not met. Participants expressed they would feel annoyance (P1, P3, P4, P5, P6), apprehension (P2, P3) acceptance (P2, P6), anger (P4), sadness (P4), violation (P4), surprise (P6) indifference (P1), and fear (P1) if their pointing data sharing preferences were not met. Annoyance was projected most often by participants (20 instances), followed by apprehension (8 instances). Participants expressed that they would feel fear (P1), apprehension (P2), and annoyance (P3, P4, P5, P6) if their typing data

were accessed by insurance companies. Besides P6 who would be accepting to employer access of her pointing data, participants expressed that they would feel fear and terror (P1), apprehension (P2, P3), violated (P4), and annoyed (P4, P5) if their employer accessed their typing data.

Exploring Privacy Standards: How Should Adaptive Assistive Technologies Handle My Data?

Participants were asked to use existing privacy standards, and/or make their own rules to guide how their data is handled by adaptive assistive technologies. We asked participants to discuss what standards they wanted to guide how their data is handled in both assistive typing and assistive pointing applications.

	P1		**P2**		**P3**		**P4**		**P5**		**P6**	
Typing (T) Pointing (P)	**T**	**P**	**T**	**P**	**T**	**P**	**T**	**P**	**T**	**P**	**T**	**P**
HIPAA	N	N	N	N	N	N	Y	Y	N	N	Y	Y
GDPR	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y
Privacy Policy	Y	Y	Y	N	Y	Y	Y	Y	N	N	N	N
Data Use Agreement	N	N	N	N	Y	Y	Y	Y	N	N	Y	Y
Terms of Service	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
My Custom Rules	Y	Y	Y	Y	N	Y	Y	Y	N	N	Y	Y
No Rules	N	N	N	N	N	N	N	N	N	N	N	N

Table 7. A table summarizing data regarding participant preferences for privacy standards guiding how adaptive assistive technologies handle their typing and pointing data. The columns represent the individual participant responses for the assistive typing application (T) and the assistive pointing application (P): Y=Yes, I would want this standard, N=No, I would not want this standard. The rows indicate the standard in question. All participants chose two or more standards to guide how their data is handled in both assistive typing and pointing applications.

All participants selected two or more privacy standards to guide how their data is collected in both assistive typing and assistive pointing applications (Table 7). None of the participants preferred adaptive assistive technologies to operate without any privacy standards or rules. Participants chose a minimum number of two standards (P1, P2, P5), and chose a maximum of all six provided data sharing standards (P4). The median number of selected privacy standards amongst participants was three.

Health Information Portability and Accountability Act (HIPAA)

Four participants did not choose for the adaptive assistive technologies to abide by HIPAA (P1, P2, P3, P5), while two of the participants wanted the applications to abide by HIPAA (P4, P6). Participants expressed polarized perspectives regarding HIPAA. Two of the participants, who had not selected HIPAA, discussed their previous experiences that had led them to view the health data protection standard as cumbersome (P1, P3):

> *"I think HIPAA is too confining sometimes. I'm going through [HIPAA restrictions] with my sister. [I want] something one step down from HIPAA." -P1*

> *"I often find HIPAA a problem...if I visit my Urologist and I got a General Practitioner and a Doctor, I would like it so that if I visit one of those practitioners, those results get shared with the rest of the medical family. What I have to do [under HIPAA] is send it to the person, for example, who ordered the test…[and] if I want somebody else to get that, other than the original agency, I've got to fill out a form, provide contact information and all, sign it… It isn't every time that I want to fill out four or five of those forms." -P3*

The other two participants, who did not select HIPAA, viewed it as irrelevant in the consideration of protecting pointing and typing data (P2, P5):

> *"If you want to do something with your health insurance, that's where HIPAA comes in." -P2*

Alternatively, two participants were enthusiastic about adaptive assistive technologies abiding by HIPAA (P4, P6):

> *"I think the HIPAA law is producing some good restraints on how the data [is accessed] already." -P6*

> *"That's a given because it's very important [in protecting my health data]." -P4*

General Data Protection Regulation (GDPR)

Four participants wanted adaptive assistive technologies in both scenarios to abide by the GDPR (P3, P4, P5, P6), while two of the participants did not select this standard (P1, P2). Participants who chose this standard favored its sensibility, and felt that it gave them agency over their data:

> *"I feel comfortable with [the GDPR] in that the focus is as much there on the user's right to inquire or raise issues with the group, so I would like that." -P3*

> *"The GDPR seems simple and sensible. If you're wondering what's going on, you can ask them." -P5*

> *"I like this.. The main thing that jumps out is that the company has to tell you what data it currently has, because you wonder, 'Well, what does it collect? What's out there about me?" -P6*

The two participants who did not select the GDPR (P1, P2) alluded to unfamiliarity with the standard as reason for omission:

> *"I don't know anything about this." -P1*

> *"I think Facebook does this, allows you to download everything they know about you.. but I'm not sure" -P2*

Privacy Policy, Data Use Agreement, and Terms of Service | My Custom Rules

All participants selected at least one of the provided agreements and disclosures in both scenarios. Half of the participants selected one of the agreement/disclosure standards (P1, P2, P5), while the other half chose a combination of these standards to be practiced by adaptive assistive technologies (P3, P4, P6). In consideration of participants' provided interpretations of these standards, we place precedence on the data protection sought by our participants in their selection, rather than the standard itself. Furthermore, participants often rationalized their selection based on a mental model of receiving more data protection than may be typically given with these standards, or choosing the standard and vocalizing a number of desired caveats, or custom standards. For example, P2 selected a privacy policy with the added caveat that it stipulate his data would remain anonymous and inaccessible by any third parties. In another session, P5 chose a terms of service agreement over a privacy policy justifying:

> *"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. Basically, I would prefer that [data sharing agreements] are out of the Terms of Service and if they want it, they can ask me. I can say, 'Okay, for the next three months you can collect it." -P5*

In this instance, P5 favored the consensual nature of the terms of service agreement, but desired agency over his collected data. He even provides an example of setting a timeframe in which an approved party can access his data.

P3 desired a nested data use agreement within a privacy policy, but also wanted these articles to offer him an active role in the decision making regarding access to his personal data:

> *"I think the main thing that strikes me, is I would 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." -P3*

P4 desired a privacy policy that would provide transparency with why and how her data would be used:

> *"I'd want [the privacy policy to disclose]: Why do they need my data, and what are they using it for?" -P4*

In summary, participants desired an active role in decision making regarding the sharing of their data, and wanted transparency from the program pertaining to why and how their data would be used.

Participatory Activity Findings

Overall, participants responded favorably to the participatory activities deployed in the second study. Participants often identified the activities as thought-provoking (P3, P4, P5, P6):

> *"This is more in-depth [than the previous interview] because it causes me to think a little more… It probably provides you with more useful data." -P6*

> *"[The activity] is a pretty good idea. It does actually make you try to think about the stuff and try to clarify your own thinking." -P5*

> *"I think [the activities] were thought-provoking for me."-P3*

> *"[The activities] were eye-opening, because you never really think about all these things as you go through life." -P4*

P4 offered that she preferred the activities to the previous interview-format study. She particularly enjoyed the tactile aspect of the activity:

> *"[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, while moving one of the cards*

We also observed instances where participants used the activity materials in creative ways. Two of our participants (P4, P5) created additional activity cards. P5 made an additional third party card representing generalized technology companies. He explained that he was not comfortable with generalized technology companies accessing his pointing data:

> *"Generalized tech companies like Google or Facebook… They have their own ends for [my data], I suppose. It may not be covered by some of these other things... 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 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 adaptive assistive technologies.

Figure 7. A photograph of P6 adapting the center line in her data sharing expectations board.

Two of our participants made use of the division line in the center of the Expectations chart (Figure 7), placing select third parties on the line and offering scenarios that could either make them feel comfortable or uncomfortable with those parties accessing their data (P3, P6).

We also witnessed participants adapting the cards as self-expression props, used synchronously with their body language. For example, in the data sharing expectations activity, P4 picked up the government third party card, announced, "*and these people*...," assertively smacked the card down into the no-access column, and chuckled.

Participants also provided constructive feedback about the activities. Two of our participants found the emotion activity to be complicated (P3, P5). P5 found it difficult to project how he would feel without having actually experienced the proposed scenarios:

> *"The hardest part is this [emotion wheel]. It's hard to tell how you would feel until you find out-- until it has happened." -P5*

P3 expressed difficulty in navigating the emotion wheel:

> *"I do find the [emotion wheel] a little bit hard to work with. 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*

The participants' criticism of the emotion wheel is consistent with recently published HCI research. Shortly after we conducted our second study, Healey et al. published research in September 2018 evaluating multiple design presentations of both Plutchik's emotion wheel and Russell's Circumplex Model of Emotion[35]. They concluded that Plutchik's model was not well-understood, and that the alternative model resonated better amongst participants. In future work, we plan to implement the model proposed by Healey et al. in our emotion activity.

6: Discussion

In this chapter, we synthesize our findings from our studies to further contextualize users' attitudes towards privacy when using adaptive assistive technologies. Participants expressed motivation to adapt assistive technologies, but also described privacy threats that corresponded to every type of threat in the LINDDUN model. We also discuss observed tensions in the space of privacy with adaptive assistive technology. These tensions include weighing the tradeoffs between performance benefits and privacy risks when using adaptive assistive technologies, and the contrasting nature of these systems as performance versus health applications.

Privacy Threat Categories and User Concerns

Using the LINDDUN model, we described theoretical privacy threats for users of AAT. Participants in our study expressed privacy concerns that can be mapped to every threat category described in our analysis. Participants were most concerned about the detectability and linkability of their AT use to medical status and saw the potential for multiple negative outcomes. For example, most participants did not want their data to be shared with employers and insurance companies. They were concerned that such exposure might lead to employment discrimination or assumptions about their other abilities (e.g., driving a car). These detectability concerns can overlap with linkability threats if the assistive technology is designed for a specific user population, for example people with ET. In this case, detecting the system on a user's computer

could imply that they are both experiencing pointing difficulties (detectability) and have ET or a similar health condition (linkability).

Participants were generally comfortable with their performance data being accessed by medical staff or family members. Interestingly, they were also comfortable with sharing their data with the assistive technology developers. Regardless of who accessed their data, participants preferred to be informed about how their data would be used (avoiding unawareness threats). Participants willingness to share their data with software developers and reluctance to share it with insurance companies or employers, reveals and attitude that may expose them to disclosure of information threats if the developers sell the data. Even in the case of research data collected by academic researchers, it is still not clear what a detailed privacy analysis would reveal about threats to protecting privacy or honoring their wish for data to not be accessed by unwanted third parties (e.g., insurance companies).

Additionally, most of the participants preferred their data to be anonymized when shared with anyone other than family members or medical staff. Several participants expressed concern about their anonymized data being de-anonymized, describing an identification threat. P3 had concerns about how installing the program might impact his wife and the system would not be able to tell them apart, signally the possibility of a non-repudiation threat when assistive technology is used on shared systems. With respect to non-compliance, one participant (P7) described the need for a review board to review and approve assistive systems and provide privacy recommendations or standards. These results show the importance of considering multiple privacy threats when designing AATs, such as PINATA, to avoid inadvertently exposing users to them.

Users Trusting Assistive Technologies with their Data

All participants were motivated to continue using computers and access the Internet. They described how pointing difficulties created barriers to access, making them enthusiastic about adaptive assistive technologies that can help bridge these barriers. While participants described a variety of concerns about privacy threats when using online non-assistive systems, no participants initially expressed concern about their personal data being collected by an assistive adaptive system. Once they were asked explicitly about who they were comfortable with accessing their assistive technology usage data, however, participants described a range of nuanced preferences, including serious concerns about privacy. Thus, there was an asymmetry in how participants perceived privacy threats with respect to non-assistive compared to assistive systems. We believe that the participants' enthusiasm towards adaptive assistive technologies might create a positive bias towards these systems that might make users overlook the privacy tradeoffs involved using them.

In discussing privacy, for example when using the LINDDUN model, the emphasis is often on the type of data that is collected and who might access this data. Our results show that another key dimension is the premise under which the data is collected. This confirms and complements previous research that showed users have negative reactions when they realize that their data was used outside of the context and beyond the premise under which it was collected [5, 85]. Users of assistive technologies might be especially vulnerable to privacy threats when their data is collected under the, often unspoken, premise of improving access for the user and others in their community.

Weighing the Privacy Tradeoffs of Adaptive Assistive Systems

Participants were aware of the benefits of an adaptive approach to assistive technology. They described how they found it important for data to be collected in a consistent manner so that the system can function more accurately. Additionally, they described how aggregating data online could improve system functionality for users other than themselves. Participants described negative reactions to potential system errors or mistakes, including frustration, resignation and even a need to seek medical attention if many mistakes were identified. Additionally, participants valued the tracking functionality of the prototype and seeing how tracking data can support self-monitoring. These attitudes contrasted sharply with the participants' privacy concerns towards non-assistive adaptive systems. While a few of the participants described neutral or benign uses of personal data collected online, most of them had serious concerns about how they might be exposed to privacy threats when using these systems. Many of these concerns were informed by news stories about data leaks on popular platforms (e.g., Facebook [80] or Yahoo [24]). These results identify an opportunity for designers of AATs to benefit from the trust and goodwill of users who might be open to sharing their personal data to improve system functionality both for themselves and for others in their community. However, there is also a danger that this trust is lost if it is betrayed by poorly designed systems that do not seriously consider the privacy concerns of users and expose them to threats.

Adaptive Assistive Technologies: Both Performance and Health Applications

There was significant ambiguity amongst our participants regarding whether or not adaptive assistive technologies collect health data. Participants often shifted their perspectives throughout the interview, reluctant to initially identify adaptive assistive technologies as explicitly collecting health data, but later offering both positive and negative scenarios alluding to the premise that these systems *could* collect user health data. Participants offered that data collected from adaptive assistive technologies could be used by medical professionals as a diagnostic tool for neurological conditions (P6) or a tool to indicate the severity of a diagnosed condition (P4), and, at the aggregate level, assist in efforts pertaining to neurology research and education for medical students (P1, P3). Some participants offered more negative scenarios, such as their collected data generating a false positive yielding an inaccurate medical diagnosis (P2, P6), or data from these systems revealing their medical conditions to unwanted third parties (P1, P6), and these unwanted disclosures resulting in being fired from a job (P1) or extrapolation of the data resulting in assumed fault by insurance companies (P1, P6).

Our participants' shifting perspectives concerning whether or not adaptive assistive technologies collect health data, illustrate the tension surrounding the perceived nature of these systems. Are adaptive assistive technologies performance applications or are they health applications? We argue that they are both performance and health applications, as performance data and other collected data can indicate health conditions ([e.g. 100]). We stress the importance of identifying these systems as both performance and health applications to clearly communicate the data collecting nature of these systems to users and support informed use of these systems.

Comparing Privacy Perspectives with Assistive Typing Verses Assistive Pointing Applications

We observed a number of differences in our participants' privacy perspectives of assistive typing compared to assistive pointing applications. Participants expected the assistive typing application to be more expansive with data collection, collecting a larger variety of personal data than the assistive pointing application. Participants were generally more open to sharing their data collected from the assistive pointing application with doctors and medical professionals and the private organization that built the program, compared to sharing their data collected from the assistive typing program with these parties. Participants identified more intense emotions when discussing how they would feel if their data sharing expectations with the assistive typing program were not met, compared to unmet data sharing expectations with the assistive pointing program.

Although participants generally viewed the assistive pointing program as more lenient in its data collecting nature, they maintained the same preferences in data sharing privacy standards for both assistive typing and pointing application scenarios. These results emphasize users' primary desire for agency over their personal data collected by adaptive assistive technologies. Future designers of adaptive assistive systems should support users by implementing customizable data collecting/sharing features that empower users to play an active role in how their data is managed.

Eliciting Attitudes Towards Privacy With Participatory Activities

The participatory activities designed for Study 2 permitted us to delve deeper into our participants' attitudes and perspectives towards privacy. Providing our participants with visual and tactile artifacts allowed our research team to visually and auditorily partake in our participants' thought processes with privacy. Participants reported the activities as thought-provoking and engaging. They interacted with the cards as props for self-expression. Participants often moved cards to different locations on the chart throughout the interview, illustrating the evolution of their thought process. The participatory activities facilitated the capturing of fluidity in our participants' perspectives, rather than their initial inclination. We implore researchers in the domain of HCI and usable privacy to consider exercising participatory methodologies to elicit attitudes towards privacy.

7: Research Implications

In this chapter, we discuss implications from our research. The chapter begins by offering usable privacy design recommendations for adaptive assistive systems. We conclude the chapter with a discussion about our future work initiatives, motivated by this research.

Recommendations

Based on our findings from both research studies, we developed two recommendations for designers, developers, and hosting sites of adaptive assistive technologies. The first design recommendation features a custom-designed icon set, representing seven key privacy features, to inform users about the privacy and data-collecting nature of an adaptive assistive technology. The second design recommendation presents a customizable data privacy settings page, designed to further inform users and give them agency over their data collected by adaptive assistive systems.

Communicating Privacy Characteristics with Icons

We asked participants about who they would be comfortable with having access to their pointing data if collected by an adaptive assistive software system. When asked if they trusted applications they had downloaded in the past, every participant responded favorably. However, every participant also expressed adamant discomfort about specific third parties (i.e. insurance companies, government, and employers) having access to their pointing data. Participants feared

that their difficulties reflected by their pointing performance might be erroneously extrapolated to other abilities such as driving a car:

> *"If they wanted to extrapolate it and say, 'she's going to hit the wrong button or the turn signal wrong... she's more likely to have an accident."-P5*

When asked about what would help them trust a new adaptive application, some participants expressed interest in a regulatory or standardization mechanism. Based on this data, we recommend developing visual mechanisms such as icons, to communicate which privacy characteristics are used in an adaptive assistive technology. These icons could be displayed on download pages of online application stores and with license agreements, to inform users about potential risks before deciding to use a system. The inclusion of icons can potentially help promote privacy policy transparency, increase privacy policy comprehension, and support user agency with respect to the disclosure of potentially sensitive personal health data. Our recommendation is in line with other emerging visual mechanisms, such as nutrition labels and comic strips [90, 45], for general privacy policy communication.

Key Privacy Characteristics of Adaptive Systems

Participants were concerned about their performance data being collected, used and shared with third-parties, without their consent. We identified seven privacy characteristics that users should be informed about when choosing adaptive assistive systems. We present a set of icons to inform users about these characteristics (Figure 8).

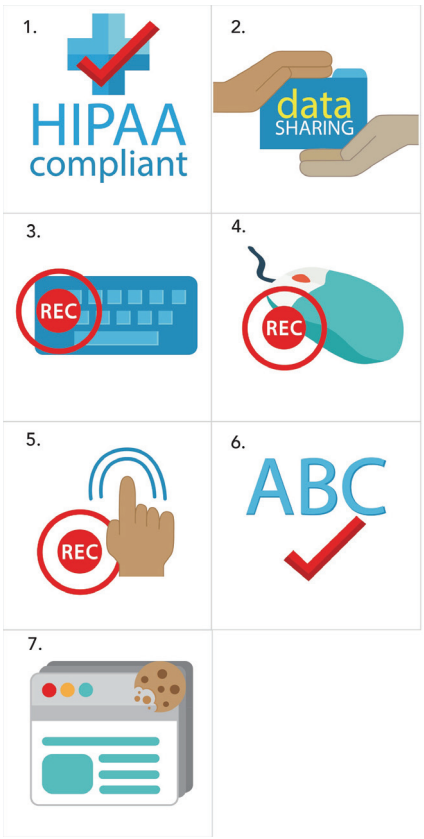


Figure 8. Icon set showing key privacy characteristics of adaptive assistive systems: 1. HIPAA Compliance, 2. Data Sharing with Third Parties, 3. Keystroke Logging, 4. Cursor and Touch Logging, 5. Gesture Logging, 6. Autocorrect Use, and 7. Cookie Use

HIPAA

Several participants interpreted our technology probe as a health application since it is designed to help users with pointing difficulties. This interpretation can lead to the assumption that a system is HIPAA-compliant (Health Insurance Portability and Accountability Act) [95] which might not be the case. We recommend that users are informed if collected data is protected.

Data Sharing with Third Parties

Participants were concerned about who has access to their data and whether it would be shared with third-parties, such as insurance companies, government organizations, and employers. We recommend that adaptive systems clearly illustrate when data is shared.

Keystroke, Cursor, Touch, and Gesture Logging

While valuable to assess ability, interaction logging (of keystrokes, cursors and gestures) can pose privacy threats to users. Analysis of this data can reveal user activity and performance that can be used to identify and link them to potentially sensitive health data. We recommend indicating the specific type of data logging performed by a system.

Autocorrect Use

Autocorrect use within an application permits the program to collect text input data. Repeated mistakes or errors of a specific nature could potentially link a user with a physical or cognitive health condition.

Cookie Use

Cookies store data about a user's online activity from an application or website on a user's device. The use of cookies can also pose a privacy threat to sensitive data collected on an adaptive assistive application.

Customizable Data Settings for Adaptive Assistive Technologies

It has been stressed that the ideal way to give individuals autonomy over their privacy, is to give them agency over how their personal information is used [34]. In both studies, we observed our participants offering varying ideas about what data should be collected, how their data should be used, and who should have access to their personal data collected from an adaptive assistive system. No particular perspective holds more validity over the other, as all users should have the ability to exercise their distinct attitudes towards privacy when interacting with systems that collect their personal data. We maintain that disparity between users' attitudes about privacy is the fundamental driving force behind privacy itself-- privacy is unique to the individual and to feel control over one's personal privacy, one must be given reigns over their data. Therefore, we should not merely make generalizations about a population's privacy preferences and apply blanket privacy provisions to adaptive assistive technologies. We should instead use this input as guidance to develop user-friendly, malleable data privacy settings that can be easily customized by system users.

To give users of adaptive assistive systems control over their data, we recommend human-centered data privacy design solutions that give users agency over what data is collected, who it is shared with, and an explanation of why the data is being requested. Based on participant input from the participatory privacy elicitation activity in Study 2, we present a privacy setting design recommendation (Figure 9), based on our PINATA design probe, that is designed to give users agency over their personal data.

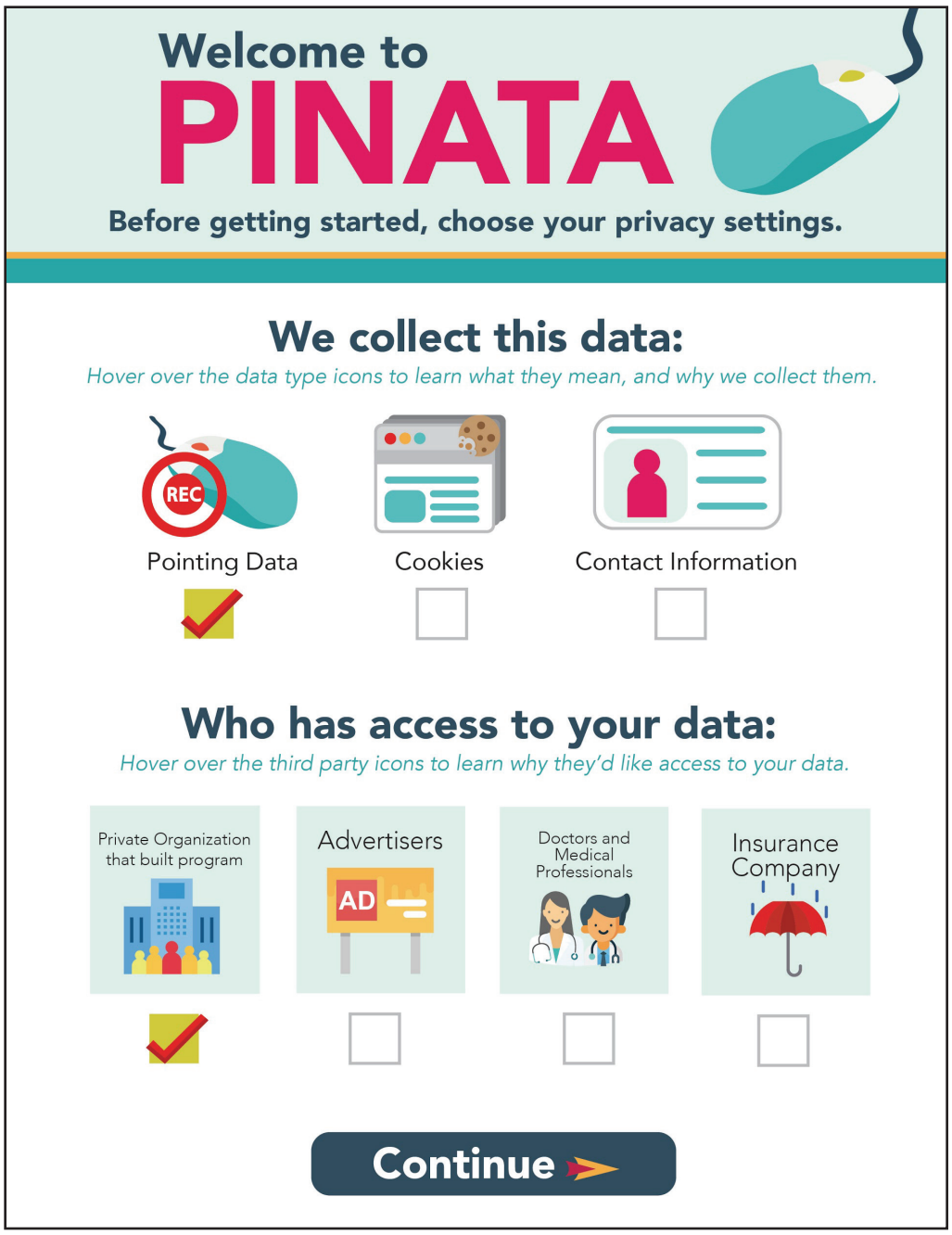


Figure 9. Adaptive assistive technology customizable privacy settings page design recommendation. We designed a privacy setting interface for the PINATA design probe that would be displayed to users upon first use after first downloading the application.

This data privacy settings page would be deployed to users upon first use of the program, and easily accessible on the program's main interface. The page would clearly depict what types of data are collected by the program, and what parties are given access to their data. The interface

would offer users the ability to hover over the data type icons to learn what these data types are and why they are collected by the application. For data types that are not critical to the functionality of the program, there would then be a check box under these data type icons to allow users to choose whether or not these data types are collected. In our design recommendation, users cannot uncheck the pointing data box, because PINATA's functionality is dependent upon the collection of users' pointing data. However, users can choose for the system to collect cookies for added functionality of performance data analysis specific to the sites they have visited, or they can choose to opt out of this data collection. Users would also be able to view what parties have access to data collected from the adaptive assistive program, and how they use their data.

Informing Users about the Data-Collecting Nature of an Adaptive Assistive System

The implementation of a data privacy settings page, deployed to users upon first use of the system, would serve as an educational tool about the data-collecting nature of the system. Furthermore, our design recommendation informs users about what data is collected, the explicit nature of that data, and how that data is used. Data from Study 2 motivated our design with the intent to inform, as participants wanted to know what data was being collected by the application:

> *"I wonder, well, what [data] does [the system] collect, or what's out there about me?" - P6, Study 2*

We chose to use hover descriptions with simple language to inform users about the explicit nature of data types collected by the system, as some participants in Study 2 admitted that they did not understand the technical data type terms:

> *"I don't even know what cookies are." - P4, Study 2*
>
> *"Cookies... I don't understand!" - P1, Study 2*

The hover descriptions would also provide an explanation of why this data was being collected, and why particular third parties wanted access to their user data, as participants in Study 2 expressed wanting to know why their data was being accessed:

> *"I think the main thing that strikes me, is I would want to know the purpose and intent of [third parties'] interest in having that data available." - P2, Study 2*
>
> *"Why do they need [my data] and what are they using it for?" - P4, Study 2*

<u>*Human-Centered Design for Data Privacy Settings*</u>

We recommend utilizing simple language and consolidating users' data privacy information into one screen with minimal scrolling:

> *"I'd like a really slimmed down privacy policy in fifth grade English, because sometimes what I find is that there is a lot of repetition from what I'm sure is a lawyer's perspective... On the other hand, to a person you're providing information, it is more confusing than enlightening in terms of what rights and options I might have." -P3, Study 2*
>
> *"I want [the privacy agreement] broken down and in everyday language... and maybe more than one box to check before you go forward."-P6, Study 2*

The Right to Choose: Giving Users Agency Over their Data

We recommend giving users of adaptive assistive technologies the ability to make informed decisions concerning what elements of their personal data is collected, and who can access that data:

> *"[I want] to be able to evaluate [parties] on each individual case, rather than grant blanket permission." - P3, Study 2*

The customization tool should be visible on the main interface of the program, permitting users to easily make changes to their data settings as their privacy attitudes change and for additional control over their data:

> *"I can say, 'Okay, for the next three months you can collect [my data]." -P5*

Future Work

In the future, we plan to study PINATA's use in the wild and update our LINDUNN analysis accordingly. Additionally, we plan to conduct formal analysis on other existing adaptive assistive systems. Our studies focused on the participants' first impressions about privacy threats when interacting with an adaptive assistive technology. In the future, we plan to conduct a longitudinal study to investigate participants' perspectives after interacting with PINATA over an extended period of time.

Finally, we intend to use the Participatory Privacy Elicitation methodology from Study 2 to contribute to the third wave of privacy, by exploring attitudes and perspectives towards privacy

within different underrepresented subpopulations. We plan to make improvements to the emotion activity by implementing the recently tested model proposed by Healey et al.[35].

8: Conclusion

Using adaptive assistive technologies that customize their functionality or appearance dynamically based on user performance, can be beneficial for people with disabilities who each have unique abilities that might also change over time. Despite their benefits, these technologies might expose users to a variety of privacy threats. We investigated these privacy threats using a LINDDUN threat model and input from end-users considering using an adaptive assistive technology. Our analysis identified six different categories of privacy threats that users might be exposed to. We contextualized these using an interview study in which we asked participants who experience pointing difficulties about their privacy concerns when selecting and using adaptive assistive technologies. Six months later, we conducted a second study with six of our participants from Study 2 where we deployed a novel participatory methodology for exploring privacy-related perspectives.

Participants had positive attitudes towards using these systems but also described privacy concerns that corresponded to every type of threat within the LINDDUN model. Participants exhibited strong preferences for who should have access to their collected data, and what data privacy standards should be implemented in adaptive assistive technologies. Participants expressed specific concerns about using AAT, and were mostly concerned about their data being used and shared without their consent. Participants often conveyed that they had felt a lack of agency in controlling their personal data when using online AATs. Despite these privacy concerns, participants were motivated to use adaptive assistive technologies to overcome accessibility barriers resulting from pointing difficulties. Participants were enthusiastic about

using PINATA, the assistive pointing application. They valued system accuracy and wanted access to their own collected data to reflect on their pointing performance. Most participants were comfortable with their data being used for medical research or to improve system accuracy, but not for screening or other unknown purposes. Most participants were comfortable with application developers and medical doctors accessing their pointing data, compared to sharing their typing data with these parties.They were hesitant about sharing their pointing data with employers, insurance companies, or governments. When giving permission to use their data, participants wanted to know how and under what premise it was used.

Participants generally expected the assistive typing application to be more expansive with data collection than the assistive pointing application. Most participants did not initially identify health data as information that would be collected by AATs, but often shifted perspectives on this matter throughout the studies. Compared to Study 1, all participants experienced changes in their pointing data sharing preferences, reflecting the dynamic nature of privacy preferences. Participants generally identified more intense emotions when discussing unmet expectations with their typing data compared to their pointing data. All participants chose at least two privacy standards to guide how their data is handled in AATs, reflecting their willingness to have agency over their data. Overall, participants found the novel participatory privacy activities thought-provoking, enjoyed the tactile aspect of the activities, and used the materials in creative ways. These findings motivate the need for the further study of privacy threats that people with disabilities might face when using adaptive assistive technologies.

Appendices

Appendix A: Study 1 Finalized Interview Protocol

1. Introduction

Hi, my name is _____. I am part of a research team from UMBC that is conducting research to better understand user expectations of online adaptive systems. Adaptive systems detect and accommodate the user's behavior; During our session, we will explore adaptive interfaces for individuals who experience pointing problems.

Before we begin, I am going to review the consent form with you.

Present Consent form

Do you have any questions before we begin?

2. Background Survey

We will begin our session with a brief background survey.

Demographics

1. What is your age?
2. What is your gender?

3. Describe your employment background.
4. Are you currently employed?
   4B. If Yes, describe your current employment.

5. General Device Usage

Do you regularly use a Desktop Computer?
(IF YES) Do you browse the internet on a Desktop Computer?

Do you regularly use a Laptop Computer?
(IF YES) Do you browse the internet on a Laptop Computer?

Do you regularly use a Touch-based Tablet (iPad, Nexus, Kindle, Nook, Surface)?
(IF YES) Do you browse the internet on a Tablet?

Do you regularly use a Smartphone (iPhone, Android)?
(IF YES) Do you browse the internet on a Smartphone?

Do you regularly use another Cell Phone (like a Flip Phone)?
(IF YES) Do you browse the internet on the Cell Phone?

6. Pointing Device Usage

Do you regularly use a Computer Mouse?
Do you regularly use a Touch Screen?
Do you regularly use a Trackpad?

7. Roughly, how much time do you spend on the internet per week?
8. How often do you browse the Internet each day?
9. Do you sometimes browse the Internet on a shared computer or device (e.g. family computer, library computer)?
10. Did you use computers in your work in the past? Please explain.
11. Do you use computers in your work now? Please explain.
12. How essential is the use of computers for you?

☐ Very Essential; I use computers often

☐ Somewhat Essential; I sometimes use computers

☐ Not Essential; I rarely or never use computers

13. How essential is the use of the internet for you?

☐ Very Essential; I use the internet often

☐ Somewhat Essential; I sometimes use the internet

☐ Not Essential; I rarely or never use the internet

Pointing Difficulties

14. Please briefly share any limitations or injuries (e.g. pain, weakness, numbness, surgery) affecting your hands or arms.
15. Would you consider yourself to have a tremor in your hands or fingers?
16. Can you perform delicate tasks with your hands (such as writing the alphabet with a pen) for extended periods of time without pain?
17. Do you sometimes find it challenging to use a pointing device (e.g. computer mouse, touchscreen or trackpad)?
    If yes, please describe the challenges.
18. The next set of questions, I will ask you to describe your level of difficulty when using the different pointing devices. Please respond with no difficulty, some difficulty, great difficulty, or "I don't use this device"

	No Difficulty	Some Difficulty	Great Difficulty	I do not use this device
Describe your difficulty using a Computer mouse	☐	☐	☐	☐
Describe your difficulty using a Computer Trackpad	☐	☐	☐	☐
Describe your difficulty using a Touch-screen	☐	☐	☐	☐

19. If you selected **Some Difficulty** or **Great Difficulty** for any of the devices, please describe your challenges/difficulties.
20. How often do you find it challenging to do the following when using a pointing device (e.g. a computer mouse, a track pad, a touchscreen).

	Never	Sometimes	All the Time
How often do you find it challenging to Click on an item (e.g. a link)	☐	☐	☐
How often do you find it challenging to Double click on an item (e.g. a link)	☐	☐	☐
How often do you find it challenging to Keep your hand steady when navigating	☐	☐	☐
How often do you find it challenging to Move the cursor in the right/desired direction	☐	☐	☐
How often do you find it challenging to Keep the mouse on the mouse pad	☐	☐	☐
How often do you find it challenging to Change directions when navigating	☐	☐	☐

21. How often do you do the following when using a pointing device (e.g. a computer mouse, a track pad, a touchscreen).

	Never	Sometimes	All the Time
How often do you Select both mouse buttons when clicking	☐	☐	☐
How often do you Accidentally click when you did not mean to	☐	☐	☐
How often do you Slip off an item (e.g. menu item) when clicking	☐	☐	☐

How often do you Overshoot or miss an item (e.g. link or button) with the cursor	☐	☐	☐
How often do you Lose the cursor	☐	☐	☐

22. Do you have any physical limitations, disability, or impairment that may make it difficult to use a pointing device (e.g. computer mouse, touchscreen or trackpad)?
    If yes, please describe them.

23. Do you have any health conditions (e.g. arthritis, nerve damage) that may make it difficult to use a pointing device (e.g. computer mouse, touchscreen or trackpad)?
    If yes, please describe them.

Background Survey ends

3. Computer Application Trust

Now we are going to change gears a bit, and discuss your level of trust with computer applications:

- How often do you download and install applications from the Internet on your phone, computer, or tablet?
- What types of applications have you downloaded?
- Do you trust these applications?
- Have you ever been suspicious of an application you installed? If so, can you tell me details about the circumstances?
- Do you have any concerns about your online privacy?
    - If "yes", can you describe your concerns?
- Do you trust an application with your data more or less when it is free?
    - Why?

4. Perceptions of adaptive interfaces

The next set of questions involve your perception of adaptive interfaces. *Adaptive systems* collect user information when navigating the web and use it to make recommendations or change their appearance and functionality based on that. For example, Amazon collects data about items you buy or browse and suggests similar items. (Some users like this feature because it helps them find items they like and other people don't like it because they are concerned that Amazon will use the collected data without their permission.)

- Have you used (these kinds of) adaptive systems before?
    - If yes, which systems?
- What is your reaction to these types of systems?
- What data do you think might be collected from this type of system?
- Who might be interested in this data, and what would they want to use it for?

5. PINATA

We're now going to focus on a specific adaptive system; PINATA is an adaptive application that changes the functionally of your cursor when using the internet. It is an extension of your internet browser that detects pointing difficulties when trying to select small objects on a website and increases the size of your cursor. It works by collecting and analyzing your data over time. You can view the collected data using visualizations.

5.A Assistance

In the interface, the bubble cursor changes size to help the user navigate on the web.

Demo PINATA - Allow user to navigate with PINATA on webpage

- What is your first impression about this type of assistance?

Show example of each assistance setting (i.e. deployed, adapt, deactivated)

- Would you prefer the bubble cursor to be activated manually or automatically?
- Would you prefer the bubble cursor to be automatically be disabled when you don't need it?

5.C Visualizations

Show the data visualizations and describe how they track a user information over time.

- What do you see in the time series visualization?
- What do you see in the website visualization?
- How would you use this data visualization?

5.D Privacy

- Are you comfortable with your data being collected by the program?
- From the following groups, who would you be comfortable with seeing your pointing data extracted from an adaptive system like PINATA?
  - -Family members
  - -Doctor/medical professional
  - -Employer
  - -Insurance company
  - -Government
  - -Private company that built the application
- Would you give permission to any of the above parties to use your data?
- Would you give permission to any of the above parties to use your data if it was anonymized?
- What degree of control would you like to have over the system's use of your data?
- Would you want it to:
  - Keep your data only on your computer (and not send it over the internet)?
  - Keep you data on a secure online website?

- Allow you to clear or edit your data?
- Not use your data at all?

- How would you like the software to assure you that your data is used in the way described above?
- Imagine PINATA was provided under two possible cases. In case 1, it will keep your data private but will cost money. In case 2, it will use your data but is free. Which condition would you prefer? Which case would you choose?

5.E. Overall Attitude and Perception towards PINATA

- What are your positive or negative thoughts about PINATA?
- Would you use PINATA or a similar system? Why or why not?
- Would you recommend PINATA to a friend?
- Do you think PINATA can be helpful (to you or others)?
- Do you think PINATA can be accurate or reliable (for you or others)?
- Do you think PINATA can adapt to your performance?
- What if this system makes mistakes?
- How would you feel if PINATA didn't detect your pointing problems?
- How would you feel if PINATA detected problems that were not there?
- How should PINATA inform you if it makes a mistake?
- Would you prefer to have a measure of accuracy or a disclosure if the system might make mistakes?

6. Final Thoughts
Please share with us if you have any other thoughts or comments.
This concludes the study. The feedback you have provided is extremely valuable--thank you so much for participating!
Present Receipt for Funds

Appendix B: Study 2 Finalized Interview/Activity Protocol

1. Introduction
Hi, my name is_____. I am part of a research team from UMBC that is conducting research to better understand user expectations of privacy for online adaptive systems.
Before we begin, I am going to review the consent form with you.

Present Consent form

Do you have any questions before we begin?

SCENARIO 1 - STAGE 1 PRIVACY EXPECTATIONS

In our previous session, we discussed how some online applications can change their functions to accommodate a user's unique behaviors. We listed some of these examples like Amazon's homepage populating items based on what a customer has purchased, and the PINATA prototype which collects a user's pointing data to adjust to a user's distinct pointing needs. To learn more about your expectations of these applications, we are going to begin by participating in an elicitation activity. We've found that this activity helps generate consistency in our interview format. In the activity, I will present a scenario involving an adaptive assistive technology. Let's begin.

Place scenario 1 in front of participant

In the first scenario, SuperSpeller is an adaptive Spell Check application that you can use on your home computer. It works by monitoring your typing.

**Demo Grammarly as an example: https://www.grammarly.com/?q=brand&utm_source=google&utm_medium=cpc&utm_campaign=brand_f2&utm_content=76996511166&utm_term=grammarly%20demo&matchtype=e&placement=&network=g&gclid=EAIaIQobChMI7uHC5Oe_3QIVnIKzCh0o6gGcEAAYASAAEgIYMvD_BwE*

What types of data do you expect to be collected by SuperSpeller to function?

Would you expect any of these data types to be collected by SuperSpeller?
Begin placing down red data type cards on table, and read name of corresponding data type

The green cards I am placing down represent different parties.

Begin placing down green cards on table, and read name of corresponding party

This chart...

Place green header 2-column chart down in front of participant

This chart is divided into two columns. The column on the left represents who you expect your typing or keystroke data to be shared with, and the column on the right represents who you do NOT expect your typing or keystroke data to be shared with.

Please take a few moments to place the green cards into either column based on who you would expect to have access to your typing data from SuperSpeller. Feel free to talk me through your expectations or ask any questions as you're going along. There are no right or wrong answers to this, as this is about your expectations of privacy when using SuperSpeller. And remember, If you don't see a card with a party you had in mind, we can add them to one of the blank cards.

Allow participant to complete activity - observe, listen, and take notes

Alright, now tell me **why you expect your typing data to be shared with these parties.**

And tell me **why you do not expect your typing data to be shared with these parties.**

We are going to come back to this chart, but first, I'm going to take a few moments to introduce the Emotion Wheel. We will be using this throughout the study so that when I ask how you would feel in a particular scenario, you will select a feeling from the Emotion Wheel that best describes how you would feel.

Show emotion wheel to participant.

For example, I might use the wheel like this: Last night, I was really excited to call my friend to give her good news, but the call was dropped three times because of the bad reception at my home.

Put blank cards down on "anticipation" and "annoyed" portions of Emotion Wheel

So, in this example, I had felt multiple emotions which you can certainly do during the study. Take some time to familiarize yourself with the Emotion Wheel, and please feel free to ask questions.

Allow participant to view emotion wheel and ask questions.

Now let's return back to the chart.

You expect your typing data from SuperSpeller to be shared with these parties. Using the emotion wheel, let's discuss how you would feel if your typing data from SuperSpeller was not shared with these parties.

How would you feel if your typing data from SuperSpeller was not shared with _____?

Repeat for each of the cards in the left column

Tell me why you would feel _____ about _____ not having access to your typing data.

Can you think of a scenario that would make you feel a more positive (or negative) emotion with _____ party not having access to your typing data from SuperSpeller?

Place cards back in left column

You do not expect your typing data from SuperSpeller to be shared with these parties. Using the emotion wheel, let's discuss how you would feel if your typing data from SuperSpeller was shared with these parties.

How would you feel if your typing data from SuperSpeller was shared with _____?

Repeat for each of the cards in the right column

Tell me why you would feel _____ about _____ having access to your typing data.

Can you think of a scenario that would make you feel a more positive (or negative) emotion with _____ party having access to your typing data from SuperSpeller?

Place cards back in right column
Move 2-column board out of the way

SCENARIO 1 - STAGE 2 STANDARDS

For the next part of this activity, we are going to discuss standards and rules that guide how your data should be handled in SuperSpeller. Standards for technologies can be implemented through laws or contracts that dictate how your data is handled. They may address data handling rules, like what data may or may not be collected and who can access this data. Standards can address how data should be handled to program developers, Internet Service Providers, Third Parties, and other stakeholders. We will discuss some of these standards shortly.

Place yellow standard strips in front of participant

These yellow strips are labeled with different standards that guide how data is managed and protected. You may or may not be familiar with some of these. I'm going to walk you through them:

- HIPAA is United States legislation that provides data privacy and security provisions for safeguarding medical information.
- The GDPR is a data protection law in the European Union. It stipulates that personal data must be processed in a lawful, fair, and transparent manner. It also gives users the right to ask a company what data it has about them, and what they company does with the information.
- A Privacy policy is a statement that discloses some or all of the ways a party gathers, uses, discloses, and manages your data.
- Terms of Service provides rules that a user agrees to before using a service.

- A Data Use Agreement is a legally binding contract used for the transfer of data that has been developed by a nonprofit, government, or private industry to an outside agency
- No Standard means no rules, laws, regulation, or contract.

Which of these standards would you want to guide how SuperSpeller handles your typing data? You can choose as few or as many standards as you would like. If the provided standards do not work for you, you can opt to create your own custom rules to regulate your typing data in SuperSpeller. Again, there are no right or wrong answers to this, as this is about your expectations of privacy when using SuperSpeller.

Why did you choose these standards to guide how SuperSpeller handles your typing data?

Why didn't you select these standards to guide how SuperSpeller handles your typing data?

Using the emotion wheel, how would you feel if the standards you selected were implemented to guide how SuperSpeller handles your typing data?

Using the emotion wheel, how would you feel if the standards you selected were not implemented to guide how SuperSpeller handles your typing data?

Bring 2-Column Chart back into focus

These are the parties you expect to have access to your typing data. **What standard should SuperSpeller abide by when sharing your typing data with these parties?** Place each card on a desired standard.

Does _____ standard change how you feel about _____ accessing your typing data?

These are the parties you DO NOT expect to have access to your typing data. **What standard should SuperSpeller abide by when sharing your typing data with these parties?** Place each card on a desired standard.

Does _____ standard being applied to Superspeller change how you feel about _____ accessing your typing data?

SCENARIO 2 - STAGE 1 PRIVACY EXPECTATIONS

Now we will move on to our second scenario. In this scenario, PINATA is an application that adapts to your changing pointing abilities, that you use at home. It works by collecting your pointing data

Demo PINATA
What types of data do you expect to be collected by PINATA?

Would you expect any of these data types to be collected by PINATA?
Begin placing down red data type cards on table, and read name of corresponding data type

We will repeat the our first activity.
Begin placing down green cards on table

Please take a few moments to place the green cards into either column based on who you would expect to have access to your pointing data from PINATA. Feel free to talk me through your expectations or ask any questions as you're going along. There are no right or wrong answers to this, as this is about your expectations of privacy when using PINATA.

And remember, If you don't see a card with a party you had in mind, we can add them to one of the blank cards.

Allow participant to complete activity - observe, listen, and take notes

Alright, now tell me **why you expect your pointing data to be shared with these parties.**

And tell me **why you do not expect your pointing data to be shared with these parties.**

Show emotion wheel to participant.

You expect your pointing data from PINATA to be shared with these parties. Using the emotion wheel, let's discuss how you would feel if your pointing data from PINATA was not shared with these parties.

How would you feel if your pointing data from PINATA was not shared with _____?

Repeat for each of the cards in the left column

Tell me why you would feel _____ about _____ not having access to your pointing data.

Can you think of a scenario that would make you feel a more positive (or negative) emotion with _____ party not having access to your pointing data from PINATA?

Place cards back in left column

You do not expect your pointing data from PINATA to be shared with these parties. Using the emotion wheel, let's discuss how you would feel if your pointing data from PINATA was shared with these parties.

How would you feel if your pointing data from PINATA was not shared with _____?

Repeat for each of the cards in the right column

Tell me why you would feel _____ about _____ having access to your pointing data.

Can you think of a scenario that would make you feel a more positive (or negative) emotion with _____ party having access to your pointing data from PINATA?

Place cards back in right column
Move 2-column board out of the way

So, we just discussed expectations of who your pointing data would and would not be shared with from PINATA. Which parties would you feel comfortable with having access to your pointing data and which parties would you feel uncomfortable with having access?

Look at results from last study

In the last study you felt comfortable with _____ accessing your pointing data.

Why do you think this has changed (or not changed)?

SCENARIO 2 - STAGE 2 STANDARDS

For the next part of this activity, we are going to discuss standards and rules that guide how your data should be handled in PINATA.

Place yellow strips in front of participant

Which of these standards would you want to guide how PINATA handles your pointing data? You can choose as few or as many standards as you'd like. If the

provided standards do not work for you, you can opt to create your own custom rules to regulate your pointing data in PINATA.

Again, there are no right or wrong answers to this, as this is about your expectations of privacy when using PINATA.

Why did you choose these standards to guide how PINATA handles your typing data?

Why didn't you select these standards to guide how PINATA handles your pointing data?

Using the emotion wheel, how would you feel if the standards you selected were not implemented to guide how PINATA handles your pointing data?

Bring 2-Column Chart back into focus

These are the parties you expect to have access to your pointing data. **What standard should PINATA abide by when sharing your pointing data with these parties?** Place each card on a desired standard.

Does _____ standard change how you feel about _____ accessing your pointing data?

These are the parties you DO NOT expect to have access to your typing data. **What standard should PINATA abide by when sharing your pointing data with these parties?** Place each card on a desired standard.

Does _____ standard being implemented by PINATA change how you feel about _____ accessing your pointing data?

Wrap Up
What are your thoughts about the elicitation activities we did today?

Would you make any changes to the activities? If so, what changes would you make?

Final Thoughts
Please share with us if you have any other thoughts or comments.

This concludes the study. The feedback you have provided is extremely valuable--thank you so much for participating!

Present Receipt for Funds

Appendix C: Study 2 Finalized Activity Materials

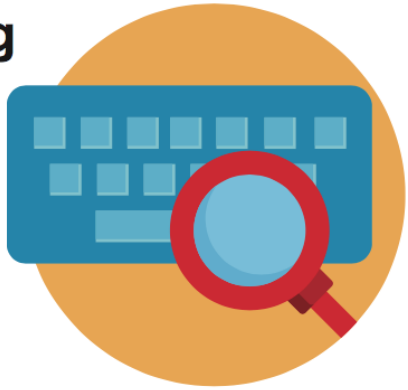
Please use the link below to access high resolution finalized privacy activity materials:
https://drive.google.com/file/d/1xdipsKpFFrzj4VwbRlTYiNVZNKG2y0N1/view?usp=sharing

Low resolution images of the finalized privacy activity materials are featured below.

A. Study Scenarios.

SCENARIO 1

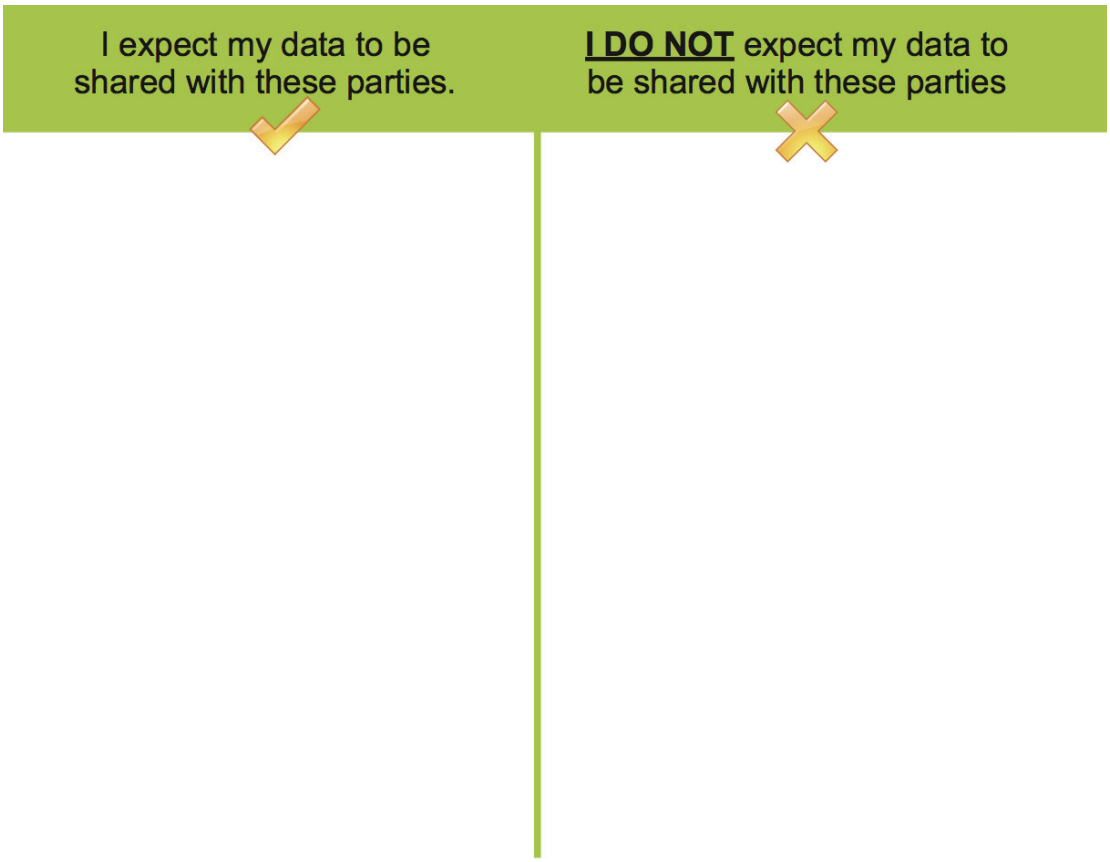
SuperSpeller is an adaptive Spell Check application that you use on your home computer.
It works by monitoring your typing.



SCENARIO 2

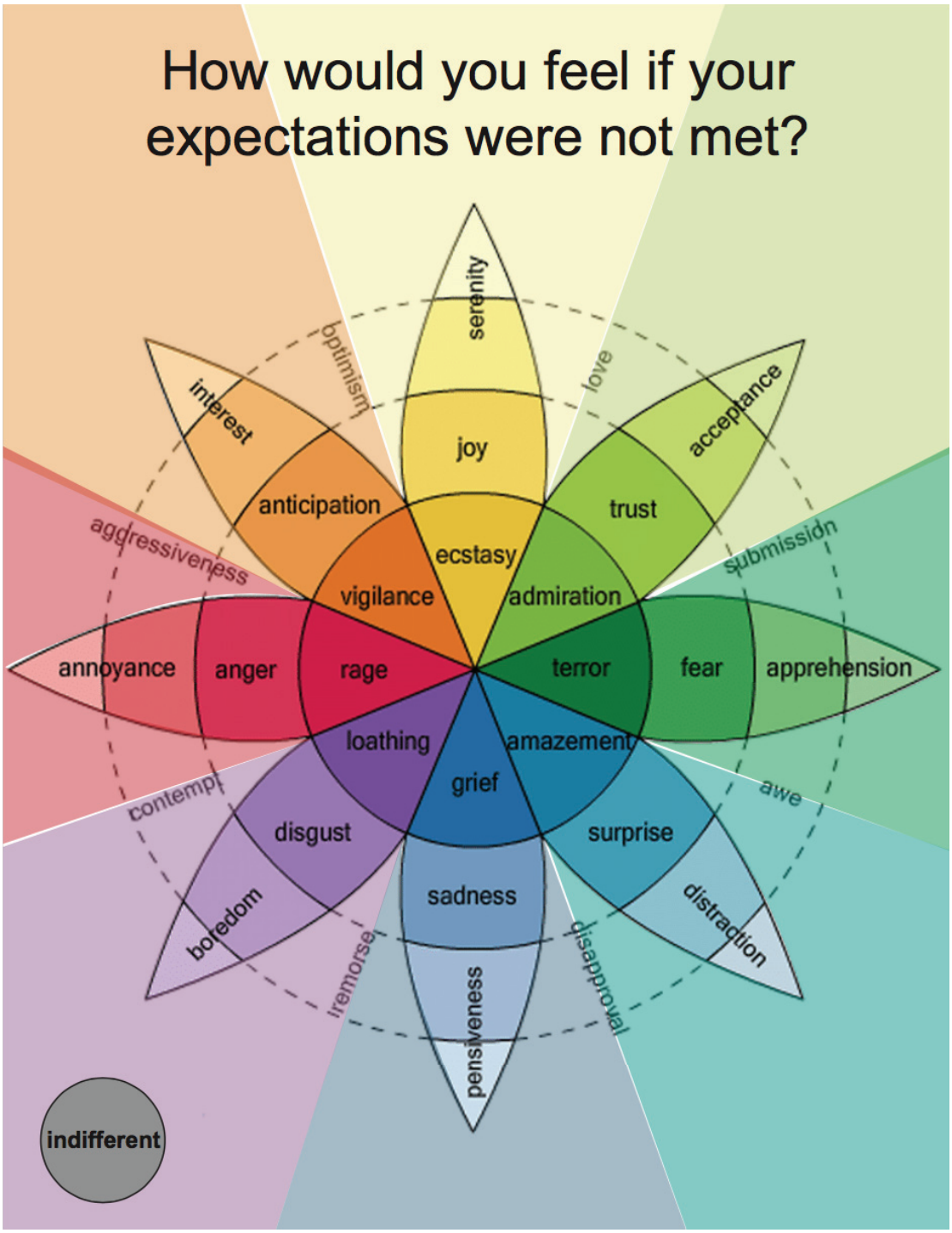
You use PINATA, an application that adapts to your changing pointing abilities, at home.
It works by collecting your pointing data.

B. Expectations Chart (Used for Stage 1 in Scenarios 1 & 2).

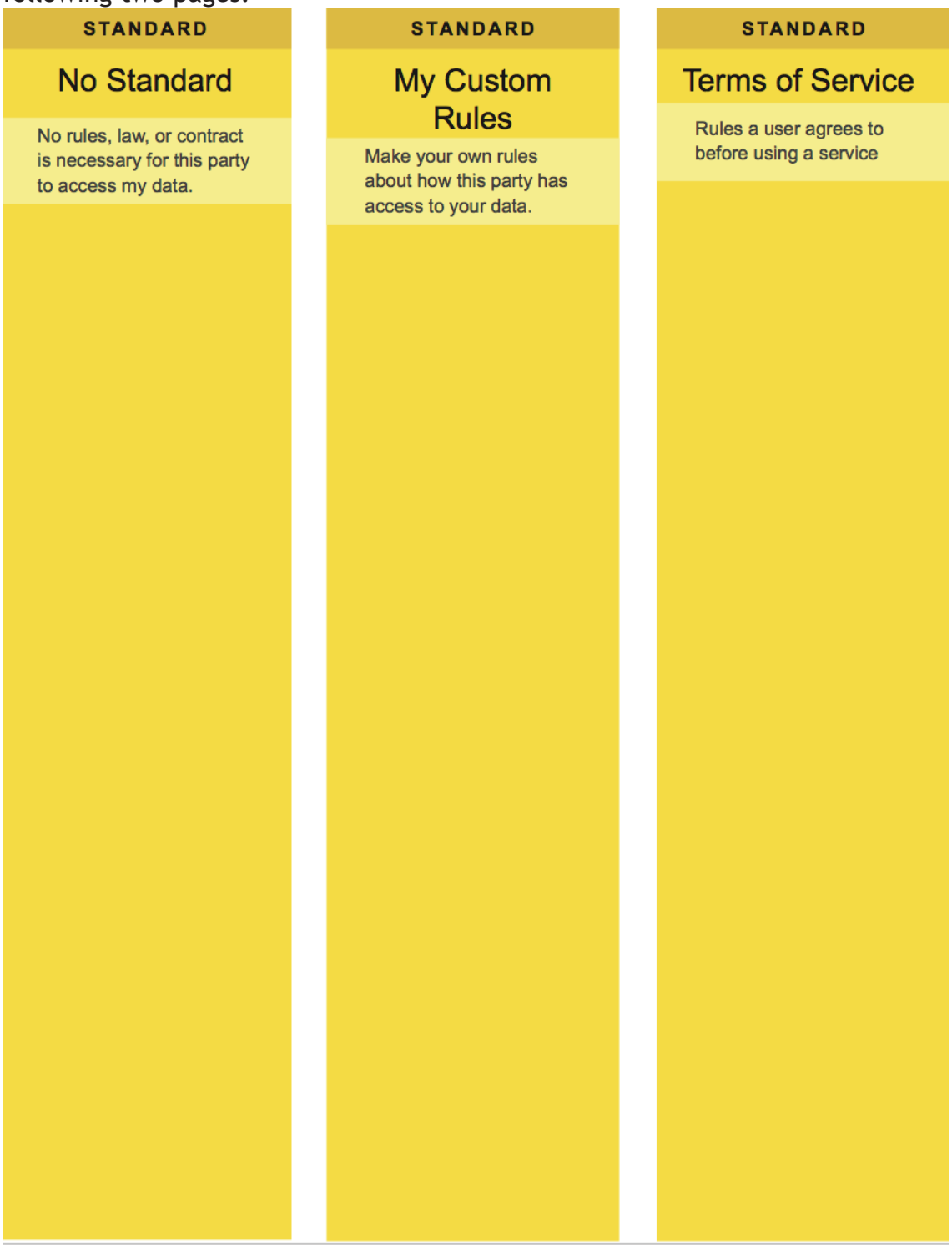


C. Green Party Cards (Used in Stages 1 and 2 in Scenarios 1 and 2). Blank cards are included for researchers or users to add additional parties if desired.

D. Plutchik's Emotion Wheel (Used in Stages 1 and 2 in Scenarios 1 and 2). [74, 75]



E. Yellow Standard Strips (Used in Stage 2 in Scenarios 1 and 2). Continued on following two pages.



STANDARD

Health Insurance Portability and Accountability Act

HIPAA is United States legislation that provides data privacy and security provisions for safeguarding medical information.

STANDARD

Privacy Policy

A Privacy policy is a statement that discloses some or all of the ways a party gathers, uses, discloses, and manages your data.

STANDARD

General Data Protection Regulation (Europe)

The GDPR stipulates that personal data must be processed in a lawful, fair, and transparent matter. It also gives users the right to ask a company what data it has about them, and what the company does with the information.

STANDARD

Data Use Agreement

a legally binding contract used for the transfer of data that has been developed by a nonprofit, government, or private industry to an outside agency

F. Red Data Type Cards (Used in Stage 1 in Scenarios 1 and 2). Blank cards are included for researchers or users to add additional data types if desired.

Bibliography

1. Ali Abdolrahmani, William Easley, Michele Williams, Stacy Branham, and Amy Hurst. 2017. Embracing Errors: Examining How Context of Use Impacts Blind Individuals' Acceptance of Navigation Aid Errors. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (CHI '17), 4158-4169.

2. Gunes Acar, Christian Eubank, Steven Englehardt, Marc Juarez, Arvind Narayanan, Claudia Diaz. 2014. The Web Never Forgets: Persistent Tracking Mechanisms in the Wild. in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, 674–689.

3. David Ahlström, Martin Hitz, and Gerhard Leitner. 2006. An evaluation of sticky and force enhanced targets in multi target situations. In Proceedings of the 4th Nordic conference on Human-computer interaction: changing roles (NordiCHI ’06), 58–67.

4. Irwin Altman. 1975. Privacy: Definitions and Properties. In I. Altman (Ed.), The Environment and Social behavior: Privacy, Personal Space, Territory, Crowding. Monterey, California: Brooks/Cole Publishing Company.

5. 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.

6. Teresa Arroyo-Gallego, María Jesus Ledesma-Carbayo, Álvaro Sánchez-Ferro, Ian Butterworth, Carlos S. Mendoza, Michele Matarazzo, Paloma Montero, Roberto Lopez-Blanco, Veronica Puertas-Martin, Rocio Trincado, and Luca Giancardo. 2017. Detection of Motor Impairment in Parkinson's Disease Via Mobile Touchscreen Typing. *IEEE Transactions on Biomedical Engineering*, 64 (9), 1994-2002.

7. Tim Baarslag, Alan T. Alan, Richard Gomer, Muddasser Alam, Charith Perera, Enrico H. Gerding, and m.c. schraefel. 2017. An automated negotiation agent for permission management. In *Proceedings of Autonomous Agents and MultiAgent Systems,* 380–390.

8. 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.

9. Anol Bhattacherjee and G. Premkumar. 2004. Understanding Changes in Belief and Attitude Toward Information Technology Usage: A Theoretical Model and Longitudinal Test. MIS Quarterly Vol. 28, 229–254.

10. 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.

11. Richard E. Boyatzis. 1998. Transforming Qualitative Information: Thematic Analysis and Code Development. Sage Publications, Inc.

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

13. Travis D. Breaux, Annie I. Antón, Kent Boucher, Merlin Dorfman. 2008. Legal Requirements, Compliance and Practice: An Industry Case Study in Accessibility. In *Proceedings of IEEE 16th International Requirements Engineering Conference* (RE'08), 43-52.

14. Alex Chaparro, Michael Bohan, Jeffery Fernandez, Sang D. Choi, and Bheem Kattel. 1999. The impact of age on computer input device use. Intl. Journal of Industrial Ergonomics, 24(5), 503–513.

15. Mira Crouch and Heather McKenzie. 2006. The logic of small samples in interview-based. Social Science Information Sur Les Sciences Sociales - SOC SCI INFORM. 45. 483-499. 10.1177/0539018406069584.

16. 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.

17. Mina Deng, Kim Wuyts, Ricardo Scandariato, Bart Preneel, and Wouter Joosen, 2011. A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. *Requirements Eng,* 16 (1), 3-32.

18. Julia B. Earp, Annie I. Antón, Lynda Aiman-Smith, and William H. Stufflebeam. 2005. Examining Internet privacy policies within the context of user privacy values. *IEEE Transactions on Engineering Management*, 52 (2), 227–237.

19. Faiella, F. & Ricciardi, M. 2015. Gamification and learning: a review of issues and research. Journal of e-Learning and Knowledge Society. 11 (3), Italian e-Learning Association.

20. 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.

21. 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.

22. Krysztof Z. Gajos, Daniel S. Weld, and Jacob O. Wobbrock. 2010. Automatically generating personalized user interfaces with Supple. *Artificial Intelligence*, 174:12-13, 910–950.

23. Luca Giancardo, Alvaro Sanchez-Ferro, Teresa Arroyo-Gallego, Ian Butterworth, Carlos S. Mendoza, Paloma Montero, Michele Matarazzo, José A. Obeso, Martha L. Gray, and R. San José Estépar. 2016. Computer keyboard interaction as an indicator of early Parkinson’s disease. *Scientific reports* 6, 34468.

24. Vindu Goel and Nicole Perlroth. Yahoo Says 1 Billion User Accounts Were Hacked. *The New York Times*. Retrieved April 11, 2018 from https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html

25. 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.

26. Grammarly. Your writing, at its best. Retrieved November 23, 2018 from https://www.grammarly.com/

27. Peter Gregor, Alan F. Newell. and Mary Zajicek. 2002. Designing for dynamic diversity: interfaces for older people. In *Proceedings of the 5th International ACM Conference on Assistive Technologies* (ASSETS '02), 151-156.

28. S. F. Gürses, C. Troncoso, and C. Diaz, "Engineering Privacy by Design", Computers, Privacy & Data Protection, 2011. Computers, Privacy & Data Protection.
14, no. 3, (2011).

29. Woodrow Hartzog. 2018. *Privacy’s Blueprint: The Battle to Control the Design of New Technologies.* Harvard University Press.

30. Foad Hamidi, Kellie Poneres, Aaron Massey and Amy Hurst. 2018. Who Should See my Data? Privacy Tradeoffs of Adaptive Assistive Technologies. In *Proceedings of the 20th International ACM SIGACCESS Conference on Computers and Accessibility* (ASSETS'18).

31. Aqueasha Martin-Hammond, Foad Hamidi, Tejas Bhalerao, Christian Ortega, Abdullah Ali, Catherine Hornback, Casey Means, Amy Hurst. 2018. Designing an Adaptive Web Navigation Interface for Users with Variable Pointing Performance. In *Proceedings of the 15th International Cross-Disciplinary Conference on Web Accessibility* (W4A '18). ACM, New York, NY, USA, Paper 16, 10 pages.

32. Aqueasha Martin-Hammond, Abdullah Ali, Casey Means, Catherine Hornback, and Amy Hurst. 2016. Supporting Awareness of Pointing Behavior among Diverse Groups. In *Proceedings of the 10th EAI International Conference on Pervasive Computing Technologies for Healthcare* (PervasiveHealth '16), 231-234.

33. 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.

34. Jim Harper. 2018. Consumer Online Privacy. CATO Institute. Retrieved from https://www.cato.org/publications/congressional-testimony/consumer-online-privacy

35. Jennifer Healey, Pete Denman, Haroon Syed, Lama Nachman, and Susanna Raj. 2018. Circles vs. Scales: An Empirical Evaluation of Emotional GUIs for Mobile Phones. In *Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services* (MobileHCI '18), 846-853. 12:1-12:11.

36. Michael Heron, Vicki Hanson, and Ian Ricketts. 2013. Accessibility Support for Older Adults with the ACCESS Framework. *International Journal of Human-Computer Interaction*, 29(11), 702-716.

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

38. Juan P. Hourcade, and Theresa R. Berkel. 2008. Simple pen interaction performance of young and older adults using handheld computers. *Interacting with Computers*, 20(1), 166–183.

39. Amy Hurst, Scott Hudson, Jennifer Mankoff, and Sheri Trewin. 2013. Distinguishing Users by Pointing Performance in Laboratory and Real-World Tasks. *ACM Trans. Accessible Computing*. 5, 2, Article 5 (October 2013), 27 pages.

40. Amy Hurst, Jennifer Mankoff, and Scott E. Hudson. 2008. Understanding pointing problems in real world computing environments. In *Proceedings of the 10th international ACM SIGACCESS conference on Computers and accessibility* (Assets '08). ACM, New York, NY, USA, 43-50.

41. Hilary Hutchinson, Mackay, W., Westerlund, B., Bederson, B, Druin, A., Plaisant, C, Beaudouin-Lafon, M., Conversy, S., Evans, H., Hansen, H., Roussel, N., and Eiderbäck, B. 2003. Technology Probes: Inspiring Design for and with Families. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI'03), 17–24.

42. Anthony Jamerson. 2008. Adaptive Interfaces and Agents. In A. Sears & J. A. Jacko (Eds.), *The human-computer interaction handbook: Fundamentals, evolving technologies and emerging applications* (2nd ed.), 433–458. Boca Raton, FL: CRC Press.

43. 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.

44. Simeon Keates and Shari Trewin. 2005. Effect of age and Parkinson's disease on cursor positioning using a mouse. In *Proceedings of the 7th International ACM SIGACCESS Conference on Computers and Accessibility* (ASSETS'05), 68-75.

45. 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.

46. Caroline J. Ketcham and George E. Stelmach. 2004. Movement Control in the Older Adult. In R. W. Pew & S. B. Van Hemel (Eds.), *National Research Council (US) Steering Committee for the Workshop for Technology for Adaptive Aging, National Academies Press*, 64-92.

47. Keith Kirkpatrick. 2016. Battling Algorithmic Bias: How do we ensure algorithms treat us fairly?, *Communications of the ACM*, 59 (10), 16-17.

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

49. Michelle N. Kwasny, Kelly E. Caine, Wendy A. Rogers, and Arthur D. Fisk. 2008. Privacy and Technology: Folk Definitions and Perspectives. In *2008 Conference on Human Factors in Computing Systems* (CHI '08), 3291-3296.

50. 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.

51. 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.

52. 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.

53. Talia Lavie and Joachim Meyer. J. 2010. Benefits and costs of adaptive user interfaces. *Int. J. Hum.-Comput. Stud.*, 68 (8), 508-524.

54. Louis Li. 2014. Adaptive click-and-cross: adapting to both abilities and task improves performance of users with impaired dexterity. In *Proceedings of the 19th international conference on Intelligent User Interfaces* (IUI '14), 299-304.

55. Xinmin Liu, Nora Hernandez, Sergey Kisselev, Aris Floratos, Ashley Sawle, Iuliana Ionita-Laza, Ruth Ottman, Elan D. Louis, and Lorraine N. Clark. 2016 Identification of candidate genes for familial early-onset essential tremor. *European Journal of Human Genetics* 24 (7), 1009-1115.

56. Elan D. Louis. 2001. Clinical practice. Essential tremor. N Engl. J. Med. 345, 887–891.

57. 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.

58. 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.

59. Keith Kirkpatrick. 2016. Battling Algorithmic Bias: How do we ensure algorithms treat us fairly?, *Communications of the ACM*, 59 (10), 16-17.

60. 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.

61. 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.

62. Aleecia M. McDonald and Lorrie F. Cranor. 2010. Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising. In *Proceedings of TPRC'10.*

63. 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.

64. Karyn Moffatt and Joanna McGrenere. 2009. Exploring Methods to Improve Pen-Based Menu Selection for Younger and Older Adults. *ACM Trans. Access. Comput.* 2, 1, A rticle 3, 34 pages.

65. Karyn Moffatt, Sandra Yuen, and Joanna McGrenere. 2008. Hover or tap?: supporting pen-based menu navigation for older adults. In *Proceedings of the International ACM SIGACCESS Conference on Computers and Accessibility* (ASSETS '08), ACM Press, 51-58.

66. Fabian Monrose and Aviel D. Rubin. 2000. Keystroke dynamics as a biometric for authentication. *Future Generation computer systems,* 16(4), 351-9.

67. Keaton Mowery and Hovav Shacham. 2012. Pixel perfect: Fingerprinting canvas in HTML5. In *Web 2.0 Workshop on Security and Privacy.*

68. Todd D. Nelson. 2005. Ageism: Prejudice Against Our Feared Future Self. Journal of Social Issues, Vol. 61, No. 2, 2005, pp. 207-221.

69. Newell, P. B. (1995) Perspectives on privacy. *Journal of Environmental Psychology* 15, 87-104.

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

71. Pew Research Center. 2017. *Automation in Everyday Life.*

72. Papert, S. (1980). Mindstorms – Children, Computers and Powerful Ideas. New York, Basic Books Inc. Publishers.

73. Parasuraman, R., Mouloua, M. And Hilburn, B. 1998, Adaptive aiding and adaptive task allocation enhance human-machine interaction, in M. W. Scerbo and M. Mouloua (eds), *Proceedings of the Third Conference on Automation Technology and Human Performance*, Norfolk, VA, USA, 119-123.

74. 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* Vol. 89, No. 4, pp. 344-350.

75. Robert Plutchik. 1994. The Psychology and Biology of Emotion. *HarperCollins College Publishers*.

76. Kellie Poneres, Foad Hamidi, Aaron Massey and Amy Hurst. 2018. Using Icons to Communicate Privacy Characteristics of Adaptive Assistive Technologies. In *Proceedings of the 20th International ACM SIGACCESS Conference on Computers and Accessibility* (ASSETS'18).

77. André Queirós, Daniel Faria, and Fernando Almeida. 2017. Strengths and Limitations of Qualitative and Quantitative Research Methods. European Journal of Education Studies. 3. 369-387. 10.5281/zenodo.887089.

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

79. Sumathi Reddy. 2018. Clues to Parkinson's and Alzheimer's From How You Use Your Computer. The Wall Street Journal. Retrieved June 19, 2018 from https://www.wsj.com/articles/clues-to-parkinsons-disease-from-how-you-use-your-computer- 1527600547

80. Matthew Rosenberg, Nicholas Confessore and Carole Cadwalladr. 2018. How Trump Consultants Exploited the Facebook Data of Millions. *The New York Times.* Retrieved April 11, 2018 from https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

81. Rothrock, L., Koubek, R., Fuchs, F., Haas, M., and Salvendy, G. 2010. Review and reappraisal of adaptive interfaces: Toward biologically inspired paradigms. *Theoretical Issues in Ergonomics Science*. 3,1 (November 2010), 47-84.

82. 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 .

83. Schön, D. (1983). The Reflective Practitioner: How Professionals Think in Action, Basic Books.

84. Andrew Sears, Min Lin, Julie Jacko, and Yan Xiao. 2003. When Computers Fade: Pervasive Computing and Situationally-Induced Impairments and Disabilities. In *Proc. of HCII’03*, 1298-1302.

85. 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.

86. Adam Shostack. 2014. *Threat Modeling: Designing for Security*. Wiley Press.

87. David Sloan, Matthew T. Atkinson, Colin Machin, and Yungqiu Li, Y. 2010. The potential of adaptive interfaces as an accessibility aid for older web users. In 88. *Proceedings of the 2010 International Cross Disciplinary Conference on Web Accessibility* (W4A‘10). Article 35, 10 pages.

89. Symantec Corporation. Internet security threat report. 19, April 2014.

90. 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.

91. Alvaro D. Taveira and Sang D. Choi. 2009. Review Study of Computer Input Devices and Older Users. *International Journal of Human-Computer Interaction*, 25(5), 455–474.

92. Shari Trewin. 2000. Configuration agents, control and privacy. In *Proceedings on the 2000 conference on Universal Usability* (CUU '00), 9-16.

93. Shari Trewin, Simeon Keates, and Karyn Moffatt. 2006. Developing steady clicks: a method of cursor assistance for people with motor impairments. In *Proceedings of the 8th International ACM SIGACCESS Conference on Computers and Accessibility,* 26-33.

94. Alexander I. Troster, Rajesh Pahwa, Julie A. Fields, Caroline M. Tanner, Kelly E. Lyons. 2005. Quality of life in essential tremor questionnaire (QUEST): development and initial validation. *Parkinsonism Relat. Disord.* 11, 367–373.

95. U.S. Department of Health & Human Services. 2017. Your Rights Under HIPAA. HHS.gov. Retrieved June 10, 2018 from https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html?language=es

96. W3C. Accessible Rich Internet Applications (WAIARIA). Retrieved June 21, 2018 from https://www.w3.org/TR/wai-aria/

97. 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.

98. Yang Wang. 2017. The Third Wave? Inclusive Privacy and Security. In *Proceedings of 2017 New Security Paradigms Workshop, Santa Cruz, CA, USA, October 1–4, 2017 (NSPW 2017)*, 9 pages. https://doi.org/10.1145/3171533.3171538

99. Westin AF. *Privacy and freedom.* New York: Atheneum; 1967.

100. Ryan W. White, P. Murali Doraiswarmy, and Eric Horvitz. 2018. Detecting neurodegenerative disorders from web search signals. npj Digital Medicine 1, Article number: 8 (2018).

101. Madhu M. Wickremaratchi, and John G. Llewelyn. 2006. Effects of ageing on touch. *Postgraduate Medical Journal*, 82(967), 301-304.

102. Jacob O. Wobbrock, Shaun K. Kane, Krzysztof Z. Gajos, Susumu Harada, and Jon Froehlich. 2011. Ability-Based Design: Concept, Principles and Examples. *ACM Trans. Access. Comput.* 3, 3, Article 9, 27 pages.

103. Wobbrock, J., Fogarty, F., Liu, S., Kimuro, S., and Harada, S. 2009. The angle mouse: target-agnostic dynamic gain adjustment based on angular deviation. In *Proc. of CHI'09*. ACM Press, 1401-1410.

104. Eileen Wood, Teena Willoughby, Alice Rushing, Lisa Bechtel, and Jessica Gilbert. 2005. Use of Computer Input Devices by Older Adults. *Journal of Applied Gerontology*, 24(5), 419–438.

105. Aileen Worden, Nef Walker, Krishna Bharat, Scott Hudson. 1997. Making computers easier for older adults to use: area cursors and sticky icons. In *Proceedings of the ACM SIGCHI Conference on Human factors in computing systems*, 266-271.

106. Kim Wuyts, Riccardo Scandariato, and Wouter Joosen, 2014. Empirical evaluation of a privacy-focused threat modeling methodology. *Journal of Systems and Software* (96), 122–138.

107. 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.