Who Should Have Access to my Pointing Data? Privacy Tradeoffs of Adaptive Assistive Technologies

Foad Hamidi, Kellie Poneres, Aaron Massey, Amy Hurst
University of Maryland, Baltimore County
Baltimore, MD, USA
{foadhamidi, kellie5, akmassey, amyhurst}@umbc.edu

ABSTRACT

Customizing assistive technologies based on user needs, abilities, and preferences is necessary for accessibility, especially for individuals whose abilities vary due to a diagnosis, medication, or other external factors. *Adaptive Assistive Technologies* (AATs) that can automatically monitor a user's current abilities and adapt functionality and appearance accordingly offer exciting solutions. However, there is an often-overlooked privacy tradeoff between usability and user privacy when designing such systems.

We present a general privacy threat model analysis of AATs and contextualize it with findings from an interview study with older adults who experience pointing problems. We found that participants had positive attitude 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 seriously consider privacy threats when designing assistive technologies to avoid exposing users to them.

Author Keywords

Assistive Technology; Adaptive Systems; Privacy; Threat Modeling; Older Adults; Essential Tremors; Pointing

ACM Classification Keywords

H.5.2. User Interfaces: User-centered Design

INTRODUCTION

Unlike physical devices, software assistive technologies can be designed to be easily customizable to meet specific user needs. For example, many software applications let users change their display settings to increase the size of text and on-screen objects to improve visibility. *Adaptive Assistive Technologies* (AATs) that collect user performance data and automatically modify their functionality offer gains in system usability and accuracy [4, 23, 45, 52]. Increasingly, these adaptive systems are connected to online servers that allow for the remote monitoring of user activity and the collection and aggregation of user data to improve overall system functionality. While the move towards connectivity and increased data collection offers 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.

In this paper, we study the tradeoffs between user privacy and assistive technology accuracy and accessibility, with a focus on adaptive systems. We focus on adaptive systems because they explicitly monitor and gather user performance data to improve system functionality. As more technologies are adopting cloud-based and Internet-of-Things (IoT) architectures that require remote processing of user data, it is crucial to study both the perceptions and attitudes of end users towards privacy when using assistive technologies, and effective methods to identify and mitigate relevant privacy threats.

Recent research has identified many online privacy threats when users' personal data is accessed and collected by remote platforms [5, 59, 62]. 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 [56]), 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 [17]). 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 [70]. This research and similar efforts that analyze keyboard [16] or touchscreen input [1] to detect disease have mostly focused on the technical aspects

ASSETS '18, October 22–24, 2018, Galway, Ireland

ACM ISBN 978-1-4503-5650-3/18/10…$15.00
https://doi.org/10.1145/3234695.3239331

of the systems. Their development, however, raise serious questions about user privacy [55].

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 [20], 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 [7, 54]. 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 [67]. 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.

Therefore, work is needed to address important and urgent research questions in this space: What privacy threats are users of assistive technologies exposed to? What do they consider when making privacy tradeoff decisions? Finally, how can designers systematically consider privacy threats when designing assistive technology systems and how can they keep the users informed about them?

To investigate these questions and understand potential risks we 1) performed a general threat model analysis of using adaptive assistive technologies and 2) conducted interviews with older adults experiencing difficulties when using a pointing device (e.g., a computer mouse). 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 [38]. 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 [7, 54]. ET is currently the most prevalent form of movement disorder in the world [39].

Our investigation revealed that there are many potential threats that users can be exposed to when interacting with software AATs. Our participants were enthusiastic towards assistive technologies that used their performance data to adapt their functionality to match user needs. However, they also expressed different degrees of concern about who might be able to access their data. The participants' positive attitudes towards assistive technologies might make them overlook some of the privacy threats that using these systems expose them to. These results underline the importance of better understanding privacy threats in the context of assistive technologies and end user's perspectives and attitudes.

The contributions of this paper are two-fold. First, we present a meta-analysis of a privacy threat model with respect to AATs to identify and categorize general privacy threats that might arise from their use. Second, we provide insights into user perceptions and attitudes towards privacy tradeoffs when choosing to use AATs. Together these 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.

RELATED WORK

Adaptive Assistive Technologies to Support Pointing

Changes in pointing ability can occur due to a range of factors, including advanced age [10, 23, 28, 29, 48, 63, 71, 74], a temporary or sustained disability [58, 65, 72] and medical conditions such as Essential Tremors (ET), Parkinson's, arthritis, or fatigue [28, 52]. These changes can make computer use difficult [10, 19, 28, 52]. In some cases, individuals are unaware of the cause of their input errors [48, 49] or changes in their abilities [9]. 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 [49]. Other individuals are aware of changes in pointing ability, but these changes occur with unpredictable frequency and severity [61, 64].

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 [45, 52, 57]. 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., [24]). Several systems have specifically

focused on helping users with pointing challenges that impact target acquisition [23, 73] and target selection [4, 57, 65, 75]. 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 [45, 47]. 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.

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, 8, 27, 59, 77]. Most of these projects focus on online marketing [5, 59] and IoT and wearable applications for health [18, 77]. 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, 59]. 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 [8, 18, 27, 77]. 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 [53].

Several projects have studied the privacy tradeoffs of health monitoring and location sensing systems for older adults [41, 69]. McNeill and colleagues conducted interviews with 20 older adults about their privacy concerns with pervasive health-monitoring systems [41]. They found that privacy was valued by their participants and important to their sense of life fulfilment. The authors recommended against ageist approaches that involve gathering extensive data to monitor older adults physical and cognitive decline at the expense of their privacy [41]. 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 [32, 33]. 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 sociotechnical issues involved in designing and deploying these systems [11, 69]. More broadly, researchers have recommended the development of multifaceted strategies that combine technical, legal and social mechanisms to develop "privacy-friendly" personalized systems [31, 35], including IoT systems for people with disabilities [22].

Understanding Risk with Privacy Threat Modeling

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 [60] 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 [12, 76], 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).

A PRIVACY THREAT MODEL FOR INPUT-BASED ADAPTIVE ASSISTIVE TECHNOLOGIES

In this section, 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 [12, 76]. We framed this analysis 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 [1, 15, 2445, 70]. 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 [70]), 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* [3, 51], 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 [50].

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) [68] 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., [45, 70]).

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 [30]. 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 [42]. When users do read these documents, they systematically misunderstand their implications for data sharing [13]. 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 [43]. 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.

Participant ID	*Age*	*Gender*	*Career History*	*Reason for Pointing Difficulty*	*Weekly Internet Use (hours)*	*Perceived Value of Internet Access*
P1	71	Female	Customer Service	Essential Tremors	2 Hours	Somewhat Valuable
P2	82	Male	Forestry	Essential Tremors	25-30	Somewhat Valuable
P3	69	Male	Geology, Computer Tech, Army, Peace Corps	Essential Tremors	30+ Hours	Very Valuable
P4	87	Male	Air Force Pilot, Computer Specialist, Accountant	Essential Tremors	8-9 Hours	Very Valuable
P5	64	Female	Computer Systems Analyst, Stay-at-Home Mom, Fitness Tech	Essential Tremors	12-14 Hours	Very Valuable
P6	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. We recruited a total of 8 participants, 7 with essential tremors and one with cataracts and impaired vision.

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 [9] 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.

INVESTIGATING USER ATTITUDES TOWARDS PRIVACY OF ADAPTIVE ASSISTIVE TECHNOLOGIES

In order to contextualize and contrast user perceptions of assistive technologies with the above threat model, we conducted interviews with eight older adults who experience variable pointing problems. Our interviews focused on experiences using technology, and perceptions of privacy online (with and without assistive technologies). In order to provide a concrete example of an AAT, we asked participants to interact with a technology probe [25] (Figures 1 and 2) that provided adaptive pointing assistance. In the following subsections, we describe our participants, materials and procedures.

Participant Demographics

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 an Essential Tremors (ET). We chose to work with this population because the effects of ET happen gradually and can impact employment and access to computers adversely. Because of these conditions, individuals experiencing ET may 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.

Adaptive Assistive Technology Probe

We developed a functional prototype of an AAT, *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.

Figure 1. The Adaptive Bubble Cursor's selection area grows in response to an increase in detected pointing errors with the larger size making it easier to select objects.

PINATA is implemented as a Chrome extension that can be installed in a users' browser and assist selecting onscreen elements. 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 [14]. 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 [45, 47].

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.

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.

Interview Procedures

We conducted eight semi-structured in-person interviews. The protocol started 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 AAT 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.

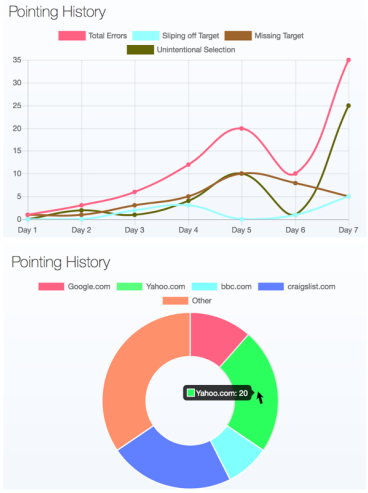

Figure 2. Pointing History Visualizations provide detected pointing error information to the user in two graphs: the *Error Type Graph* (top) shows the frequency of different kinds of error over time and the *Website Graph* (bottom) shows the most common websites where pointing errors have occurred.

Next, we asked participants about their privacy concerns with data that could be collected by PINATA. We asked how comfortable they were if they knew that their data might be accessed by six different entities: family members, medical staff, the government, insurance companies, employers, and software developers. For each entity we asked whether the participant's choices would differ if the data was anonymized (i.e., their real names and addresses were not stored along with their data on the remote server).

Participant sessions took on average 77 minutes, ranging from 62 to 92 minutes. We audio recorded and transcribed every interview, with the exception of one interview (P4), in which we took detailed notes instead at the participant's request. We conducted an iterative thematic analysis to identify and synthesize themes within the data.

FINDINGS

Staying Connected: The 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 day). 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 population platforms, such as Facebook [56].

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 AAT 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 [1]. 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. P1stated that she would probably look at the visualizations but was unsure if she was going to change her behavior based on them.

	Yes		Maybe		No	
Private (P) Anonymized (A)	**P**	**A**	**P**	**A**	**P**	**A**
Family Members	6	7	1	0	1	1
Medical Professionals	6	8	1	0	1	0
Employers	1	3	1	1	6	4
Insurance Companies	0	1	1	0	7	7
Government	1	4	1	0	6	4
Private Assistive Tech Company	5	7	2	1	1	0

Table 2. Summary of 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 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?

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 2). 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.

DISCUSSION

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 AATs 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 AATs 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, 59]. 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 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 they 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 [56] or Yahoo [17]).

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.

LIMITATIONS AND FUTURE WORK

In a formal application of LINDDUN, it is common to apply the model to a specific technology used in realistic settings. 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 assistive systems.

Our current interviews focused on the participants' first impressions about privacy threats when interacting with an AAT. In the future, we plan to conduct a longitudinal study to investigate participants' perspectives after interacting with PINATA over an extended period of time.

CONCLUSION

Using AATs 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 AAT. 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 AATs. Participants had positive attitudes towards using these systems but also described privacy concerns that corresponded to every type of threats within the LINDDUN model. These findings motivate the need for the further study of privacy threats that people with disabilities might face when using AATs.

ACKNOWLEDGMENTS

This project is funded by NIDILRR grant #-90DP0061-01-00.

REFERENCES

1. 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.
2. 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.
3. 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.
4. 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.
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. 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.
7. 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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 Managemen*t, 52 (2), 227–237.
14. 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.
15. 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.
16. 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.
17. 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
18. 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.
19. 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.
20. Woodrow Hartzog. 2018. *Privacy's Blueprint: The Battle to Control the Design of New Technologies.* Harvard University Press.

21. 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.
22. 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.
23. 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.
24. Amy Hurst, Scott E. Hudson, Jennifer Mankoff, and Shari Trewin. 2013. Distinguishing users by pointing performance in laboratory and real-world tasks. *ACM Transactions on Accessible Computing,* 5(2), 5.
25. 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.
26. 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.
27. 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.
28. 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.
29. 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.
30. Keith Kirkpatrick. 2016. Battling Algorithmic Bias: How do we ensure algorithms treat us fairly?, *Communications of the ACM*, 59 (10), 16-17.
31. Alfred Kobsa. 2007. Privacy-enhanced personalization. *Commun. ACM,* 50 (8), 24-33.
32. 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.
33. 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.
34. Talia Lavie and Joachim Meyer. J. 2010. Benefits and costs of adaptive user interfaces. *Int. J. Hum.-Comput. Stud.,* 68 (8), 508-524.
35. 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.
36. 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.
37. 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.
38. Elan D. Louis. 2001. Clinical practice. Essential tremor. *N Engl. J. Med*. 345, 887–891.
39. 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.
40. 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.
41. 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.
42. 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.
43. Aleecia M. McDonald and Lorrie F. Cranor. 2010. Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising. In *Proceedings of TPRC'10.*

44. 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,* 4, 543-568.
45. 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.
46. 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.
47. 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.
48. 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, Article 3, 34 pages.
49. 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.
50. Fabian Monrose and Aviel D. Rubin. 2000. Keystroke dynamics as a biometric for authentication. *Future Generation computer systems,* 16(4), 351-9.
51. Keaton Mowery and Hovav Shacham. 2012. Pixel perfect: Fingerprinting canvas in HTML5. In *Web 2.0 Workshop on Security and Privacy*.
52. Richard Pak, and Anne C. McLaughlin. 2010. *Designing displays for older adults.* Boca Raton, FL: CRC Press.
53. Pew Research Center. 2017. *Automation in Everyday Life*.
54. Ilkka Rautakorpi. 1978. *Essential Tremor. An Epidemiological, Clinical and Genetic Study*. Finland: Academic Dissertation University of Turku.
55. 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
56. 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
57. Ling Rothrock, Richard Koubek, Frederic Fuchs, Michael Haas, and Gavriel Salvendy. 2010. Review and reappraisal of adaptive interfaces: Toward biologically inspired paradigms. *Theoretical Issues in Ergonomics Science*, 3(1), 47-84.
58. 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.
59. 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.
60. Adam Shostack. 2014. *Threat Modeling: Designing for Security*. Wiley Press.
61. 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 *Proceedings of the 2010 International Cross Disciplinary Conference on Web Accessibility* (W4A '10). Article 35, 10 pages.
62. Symantec Corporation. Internet security threat report. 19, April 2014.
63. Alvaro D. Taveira and Sang D. Choi. 2009. Review Study of Computer Input Devices and Older Users. *Intl. Journal of Human-Computer Interaction*, 25(5), 455–474.
64. Shari Trewin. 2000. Configuration agents, control and privacy. In *Proceedings on the 2000 conference on Universal Usability* (CUU '00), 9-16.
65. 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.
66. 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.
67. U.S. Department of Health & Human Services. 2017. Your Rights Under HIPPA. *HHS.gov.* Retrieved June

10, 2018 from https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html

68. W3C. *Accessible Rich Internet Applications* (WAI-ARIA). Retrieved June 21, 2018 from https://www.w3.org/TR/wai-aria/
69. 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.
70. Ryan W. White, P. Murali Doraiswamy, and Eric Horvitz. 2018. Detecting neurodegenerative disorders from web search signals. *npj Digital Medicine* 1(1), 8.
71. Madhu M. Wickremaratchi, and John G. Llewelyn. 2006. Effects of ageing on touch. *Postgraduate Medical Journal*, 82(967), 301-304.
72. 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.
73. 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.
74. 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.
75. 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.
76. 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.
77. 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.