Decoding the Privacy Policies of Assistive Technologies

Kirk Andrew Crawford
Yi Xuan Khoo
Asha Kumar
Helena M. Mentis
Foad Hamidi
kirk4@umbc.edu
ykhoo1@umbc.edu
akumar8@umbc.edu
mentis@umbc.edu
foadhamidi@umbc.edu
University of Maryland, Baltimore County
Baltimore, Maryland, U.S.A.

ABSTRACT

As assistive technologies (ATs) have evolved, they have become increasingly connected. However, these increasing connections pose significant privacy challenges, especially when user privacy is described using complex privacy policies. Our study decodes the privacy policies of 18 ATs to understand how data collection and processing are communicated with users. We find that (1) AT privacy policies are structured to offer legal protections to their companies and not always to protect user privacy, (2) AT privacy policies are absent protections for individuals with disabilities, (3) AT policies are inconsistent when describing data storage, handling, and security methods, (4) AT policies often do not differentiate between essential and non-essential data collection, and (5) there is often a lack of transparency in AT policies around third-party data sharing. These findings reveal that AT privacy policies overlook and underestimate a user's acceptable privacy risks. We conclude our study by discussing AT design implications.

CCS CONCEPTS

• **Human-centered computing** → **Accessibility technologies**; • **Security and privacy** → *Privacy protections.*

KEYWORDS

accessibility, accessible technology, privacy, policies, software engineering

ACM Reference Format:
Kirk Andrew Crawford, Yi Xuan Khoo, Asha Kumar, Helena M. Mentis, and Foad Hamidi. 2024. Decoding the Privacy Policies of Assistive Technologies. In *The 21st International Web for All Conference (W4A '24), May 13–14, 2024, Singapore, Singapore.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3677846.3677850

W4A '24, May 13–14, 2024, Singapore, Singapore
© 2024 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-1030-8/24/05
https://doi.org/10.1145/3677846.3677850

1 INTRODUCTION

Assistive technologies (ATs) that use software, such as those designed to improve navigation for people with visual impairments [50] or pointing and typing for people with motor impairments [16], among others, increasingly collect data to enhance their functionality. For people with disabilities who rely on ATs in everyday life, the intersections of accessibility and privacy hold added challenges. For example, one's reliance on AT often necessitates sharing more than basic personal identifiable information (PII), exposing more intimate details about themselves, such as their physical and cognitive abilities or even real-time location data [16, 50, 54]. While often presented by AT designers as essential for enhanced functionality, such disclosures can inadvertently compromise an individual's privacy [2, 3]. The balance between AT function and protecting user privacy becomes increasingly challenging when this functionality necessitates sharing data with third-party companies [13, 16]. Many AT users, unaware of the risks associated with third-party data sharing [1], can harbor misconceptions about where and how their information might be accessed or exploited [21]. This limited understanding of how data is used, often due to the complexities and length of privacy policies [22, 23, 33, 52], and, for some, the lack of accessible control over information that can be shared [11], increases the risk of data misuse by companies[ibid]. Moreover, unclear or hidden data usage does little to prevent the erosion of trust between end-users and AT companies [39].

For people with disabilities, a lack of visibility into how data is shared and used by companies amplify existing vulnerabilities [28, 31, 42], such as when personal data falls into the hands of malicious actors, like an abusive partner [24, 25]. People with disabilities are particularly vulnerable to intimate partner violence (IPV), as they face nearly double the lifetime risk of IPV compared to individuals not experiencing a disability [47]. For those who rely on ATs for their daily work, the use of ATs and, consequently, the need to share personal information is often not a choice [19]. Instead, it becomes a necessity for them to fulfill their professional responsibilities [ibid]. In such scenarios, we pose that the line between the risks and benefits of data sharing and the use of ATs becomes blurred, making it challenging to discern. Consequently, while ATs address specific user needs, there is a simultaneous and equally important end-user desire for privacy [56].

Given this pertinent intersection, we pose the research question: *How do AT companies communicate the collection and processing of user data within their privacy policies?*

We analyzed the privacy policies of a range of ATs available in the United States (U.S.), focusing on those recommended by state and federal agencies, to uncover how data collection and use are publicly conveyed to end-users. Following our analysis, we first highlight several themes and opportunities for AT companies to address when writing privacy policies. Second, we argue that without a deep understanding of the unique risks and vulnerabilities faced and experienced by people with disabilities, AT companies may overlook or underestimate a user's acceptable privacy risks. Concluding our study, we offer system design suggestions for AT companies seeking to address these privacy challenges.

2 RELATED WORK

2.1 Privacy of Digital Assistive Technologies

To date, despite recognizing the importance of considering the privacy of people with disabilities when designing digital technologies, few studies have focused on the privacy of AT and accessibility applications [55]. Stangl et al. used interviews with end-users and analysis of 13 privacy policies to investigate how AT companies communicate their data collection and use practices to people with visual impairments and what happens to users' personal visual data (e.g., images and videos) [50]. They found that users' privacy concerns towards ATs depend on their understanding of how services are provided, the implications of sharing their personal visual data, and how companies adhere to their values. Their policy analysis showed that most companies did not communicate whether they retain personal visual data, no companies allowed users to opt out of personal data collection, and only two companies mentioned that they sell photos and images to other third parties. Among other implications, these findings show that AT companies currently limit users' opportunity to provide informed consent and introduce a misalignment between what end-users need to know and what the companies offer.

Other studies that focused on understanding the perspectives of end-users with disabilities towards technology privacy also found that individuals often have nuanced preferences and that it is important to find participatory and inclusive ways for them to express and recognize these preferences. For example, in a study of users who experience pointing or typing difficulties, Hamidi et al. found that participants distinguished between who they want access to their pointing vs. typing data and how third parties should use this data [16]. To facilitate discussing these preferences, the researchers developed a participatory toolkit that used printed elements to outline and distinguish between third parties, data types, and privacy regulations, among others [15]. Several other methods have been developed to elicit the privacy perspectives of vulnerable populations, including people with disabilities. These include interviews [6, 21, 57], surveys [58], focus groups [27], and co-design activities [60, 61]. For example, Ray et al. asked 20 older participants to create open-ended drawings that expressed their conceptions of the general concept of "privacy" in both digital and non-digital contexts [43]. This activity was followed by semi-structured interviews where participants elaborated on their drawings. The study revealed participants' privacy concerns, feelings of resignation and fear, and protection strategies.

In another study, Asgharpour et al. used a novel virtual card-sorting method to elicit security mental models of expert and non-experts [5]. Participants sorted 29 virtual cards with security-related words (e.g., "Spyware", "Spam") into six categories correlating to common security mental models (e.g., "Physical Safety", "Warfare"). The study revealed significant differences in mental models from these groups. So far, little work has been done on including end-users in the creation of privacy policies, as these documents are generally seen as hard for users to understand and create [36].

While these studies focus on the important perspectives of AT end-users, they do not systematically analyze the privacy policies of a diverse set of AT privacy policies to understand how they communicate their data collection and use characteristics.

2.2 Privacy Policy Analysis and Presentation Improvement

Another relevant research direction has focused on analyzing existing privacy policies to determine their quality and appropriateness for non-expert users. While privacy policies and the information contained within them differ across companies and applications, these documents are typically designed to inform end-users of the information or data the company collects and how they use what is collected. Many countries have developed privacy regulations that necessitate the inclusion of privacy policies for software applications [51]. Despite the increased necessity of including these public-facing documents, prior studies have shown the complex structure and content of existing privacy policies and their general lack of readability and accessibility for non-expert end-users [30, 33], characteristics that would cost users significant amounts of time if they were to read or even skim privacy policies [30]. This is in the face of evidence that shows that with increased transparency, privacy policies can provide increased comprehension of data collection and use practices of applications to users [29].

Previously, several research efforts have analyzed privacy policies using both qualitative and quantitative approaches, mainly focusing on readability [23, 33], while others created large databases of privacy policies for automatic analysis of text features [48, 59]. Zimmeck et al. created a tool that automatically extracted and analyzed the privacy policies of more than a million apps and found that many apps do not have privacy policies, and of those that do, more than 12% have at least one location-related potential compliance issue [63]. Researchers analyzing policies have identified several challenges, including difficulty locating and accessing policies, reading and interpreting them, and imperfections in machine-learning and crowd-based analysis approaches [35]. Despite these challenges, similar analyses of privacy policies have shown that this approach can effectively assess a company's data collection and processing practices. For example, Jensen and Potts analyzed 75 privacy policies of online websites and found that a large portion of the online user population can only reasonably be expected to understand a small fragment of the policies [18]. The researchers found the policies particularly lacking in communicating information about how users would be notified about changes. Furthermore, Reidenberg et al. found considerable variations between how experts and non-experts interpret online privacy policies, especially concerning data-sharing practices [44]. The authors argued that these discrepancies signal that privacy policies may be misleading the general public and, in their current form, can be considered unfair and deceptive [44]. While many of these approaches are created to analyze policies at scale for widely-used products, such as websites and apps, fewer studies have focused on the specific privacy needs of vulnerable populations, such as people with disabilities, and to the extent these are reflected in the privacy policies of existing products.

Researchers in this space have subsequently explored strategies for improving the accessibility of privacy policies, including formatting privacy information using a nutrition label style [22], comic-based policies [52], and different visualization variations [26], among others. Others have focused on creating tools to aid users in reading and understanding policies independently. For example, Harkous et al. used deep learning to create an application that allows both structured and free-form querying of privacy policies [17]. A demonstrated application of this approach would be a chatbot that can analyze an online privacy policy and answer a user's questions about its features. In another approach, Zaeem et al. created a tool to automatically generate a short summary of a given privacy policy for non-experts [62].

With notable exceptions (e.g., [50]), few of these previous projects have focused on AT or accessibility applications, leaving a gap in knowledge on how these policies are currently composed and presented to users. Furthermore, to our knowledge, no study has looked at the privacy policies of various ATs designed for people with different types of disabilities to assess how they communicate their characteristics to end-users. We, thus, utilized a similar process to analyze AT companies' privacy policies to determine acceptable privacy risks based on AT functionality and how these companies communicate those risks in their privacy policies.

3 RESEARCH METHODS

3.1 Data Collection

We systematically selected ATs for inclusion into our corpus by following the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) process [1], which involves four key phases: identifying sources, screening for relevance, establishing eligibility criteria, and finalizing the corpus [40].

Phase 1: Identifying sources From October 2022 to August 2023, we identified and compiled a list of over 100 ATs using publicly available AT recommendation lists curated by U.S. state [2] and federal governments[3]. Additionally, we included popular ATs reviewed in prior work [49, 50]. Our investigation focused exclusively on ATs accessible in the U.S. and those with privacy policies publicly disclosed on their respective company websites.

Phase 2: Screening for relevance We meticulously screened each AT identified in the previous phase, checking for whether each had a public and functional website.

Phase 3: Establishing eligibility criteria After conducting an exhaustive review of the AT websites and any available privacy policies, and to appropriately scope our analysis to address our research questions directly, we formulated the following criteria to determine the inclusion of ATs in the final corpus:

- AT collects, stores, analyzes, or shares user data
- AT had a functioning public website, which we could access
- AT was designed to assist individuals with visual impairments, hearing impairments, mobility challenges, cognitive differences, or speech-related challenges

Concurrently, we applied exclusion criteria to refine our list further:

- AT's privacy policy did not explicitly address privacy provisions or contained sections that were not pertinent to the goals of this study

Phase 4: Finalizing the corpus After reviewing and comparing all ATs against the inclusion and exclusion criteria, we finalized the corpus, which included 24 ATs (presented in Table 1). Notably, 6 ATs that met our inclusion criteria did not have a publicly available privacy policy (as indicated in the third column). The third author contacted the companies of these ATs to inquire about the absence of publicly accessible privacy policies and to seek details on AT privacy provisions for policies that lacked them. Additionally, the third author reached out for clarifications for companies with unclear AT privacy policies. Only one company responded to these inquiries and provided useful AT privacy details, addressing several questions about the privacy of their AT. We included this feedback for coding and analysis.

3.2 Data Analysis

We followed Braun and Clarke's thematic analysis process [7] to review and familiarize ourselves with the data, assign descriptive preliminary codes, search for candidate themes, review the candidate themes together, name the themes, and finally report the themes.

After individually reviewing the collected policies, the first three authors collaborated to inductively code one policy together to form a shared understanding of the legal language used within similar policies. They subsequently divided the review of the remaining policies, and each inductively coded the remaining data separately. They tagged the policy documents in Microsoft Word and then utilized Microsoft Excel [8] to collect all of the codes and policy snippets. During coding, regular meetings were convened among the first three authors to discuss and cross-check coding to ensure each code accurately represented the data.

Once all data were coded, the first three authors convened once again to review the codes, refining and restructuring them as necessary. Based on these codes, candidate themes were constructed and collated with data relevant to each theme. The team then followed Patton's dual criteria [41] to evaluate internal homogeneity (review of the relationships among the data and codes that inform each candidate theme) and external heterogeneity (a review of each candidate theme against the data) within each candidate theme [9]. Following these reviews, codes and candidate themes were further refined and restructured as necessary until the coders agreed that they reflected the data and were aligned with the research question.

[1] http://prisma-statement.org/
[2] https://mdod.maryland.gov/mdtap/Pages/MDTAP-Home.aspx
[3] https://www.cap.mil/

Table 1: ATs Reviewed

AT	AT Functionality Description	AT Privacy Policy Publicly Available	AT Company
MyNotifi	Fall detection device that alerts loved ones	Yes	Medhab, LLC.
Sunu Band	Mobility aid using echolocation for visually impaired	Yes	Sunu, Inc.
NovaChat8	Dynamic speech-generating device	Yes, company responded to research inquiry	PRC-Saltillo
Aira App	App and service for visual interpretation	Yes	Aira Tech Corp
Be My Eyes App	App and service for visual interpretation	Yes	Be My Eyes
Acesight	Electronic glasses for the visually impaired	Yes	Zoomax Tech, Co.
Orcam MyEye	Electronic glasses for the visually impaired	Yes	OrCam Technologies
Dragon Voice	Speech-to-text software	Yes	Nuance
Ghotit	Writing/reading apps for Dyslexia	Yes	Ghotit Ltd
TapTap See	Space recognition app for the visually impaired	Yes	TapTapSee
LookTel GPS	Navigation app for the visually impaired	Yes	NantWorks, LLC.
Supersense	Space recognition app for the visually impaired	Yes	Mediate
Envision App	Smartglasses and app for the visually impaired	Yes	Envision Tech. B.V.
IrisVision	Electronic glasses for the visually impaired	Yes	IrisVision Global
Lazarillo	Navigation maps for indoor/outdoor	Yes	Lazarillo, LLC.
Nueyes Pro	Electronic glasses for the visually impaired	Yes	NuEyes Tech, Inc.
Sightplus	VR headset for low vision users	Yes	Vision Tech. (GiveVision)
Oxsight	Electronic glasses for the visually impaired	Yes	OXSIGHT Ltd.
Medallion Mini Receiver	Alert system for people who are hard of hearing	No	SilentCall Communications
UbiDuo 3 Wireless	Wireless communication device for those who are hard of hearing	No	SComm
Orbit Chat	App to help deafblind individuals communicate	No	Orbit Research
Braille displays	Braille devices for the visually impaired	No	Humanware
Magnifiers	Devices for the visually impaired	No	Eschenbach
eSight	Electronic glasses for the visually impaired	No	eSight Corp.

These final candidate themes were subsequently reviewed among all authors. Any disagreements about codes or themes identified were addressed by revisiting the data, revising codes, and refining candidate themes until there was an agreement between all authors. Finally, the team returned to the data to identify short extracts that were used to punctuate the final theme names to ensure each theme fully and accurately communicated the findings from the data.

While coding each AT's privacy policy, the team only focused on sections or clauses of each policy detailing privacy provisions related to the ATs. Sections or clauses that pertained to broader AT company services or websites and were not specific to the AT were consciously set aside to maintain the focus of the analysis.

A sample of our final codes and their connection to the themes discussed are provided in Table 2.

3.3 Positionality

Our collective expertise extends across the domains of privacy and accessibility research, having a mix of academic and industry experiences. We do not embody the disabled experiences of end-users of the systems we have studied but have previously worked with many AT users, which may have potentially shaped our analytical lens and the outcome of our research [46]. None of the research team members have previously worked at AT companies.

4 FINDINGS

4.1 Lack of Protection for People with Disabilities

Our analysis showed that no policies provided protections specific to individuals with disabilities. This finding is surprising given the application domain of ATs, which are technologies designed specifically for users with disabilities. Several AT policies emphasized special protections for other vulnerable populations, specifically children (13 out of 18).

Dragon Voice's specific age-related privacy provisions underscored a protective stance for children:

> "...if the user is under the age of 16, Nuance may receive personal data from children under the age of 16. It is the responsibility of the Nuance customer to obtain any consents required under applicable law..." (Nuance)

This policy directly emphasizes obtaining additional consent for collecting personal data from children. However, similar protections for individuals with disabilities are absent from the policy. The omission of explicit provisions to safeguard this population is particularly notable given scenarios of severe disability that could potentially impede an individual's ability to provide informed consent themselves [12].

We found a similar omission in Supersense's policy:

> "Services do not address anyone under the age of 13....if you are a parent or guardian and you are aware that your child has provided us with personal information, please contact us..." (Mediate)

Particularly notable are Supersense's provisions for parents or guardians to contact the company should they desire their child's personal information to be removed from the company's databases. While it is important to protect underaged users, we pose that focusing on this single population overlooks the privacy needs of other vulnerable populations [32].

4.2 Legal Guardrails Protect Company

At the foundation of all privacy policies were current legal institutional guardrails. However, our analysis uncovered that these

Table 2: Sample Qualitative Thematic Codes

Theme	Codes
Lack of protection for people with disabilities	Products and services not intended to be used by children or those under 18 years of age; Protection: protections for children under the age of 16; Protection: protections for users under the age of 13; Protection: Age requirement to use service; protection of children
Legal guardrails protect company	Company protection: users' responsibility of being mindful of what information to Disclose; Company protection: Software updates without notice; Protection: company will do their best to protect data, however it's not guaranteed; Law: share data to comply with the legal process; Law: company may be required to release data as required by law; Company protection: users' responsibility of being mindful of what information to disclose
Policies inconsistent when describing data storage, handling, and security methods	Usage: ways the company uses the personal information they collect; Usage: other uses of the data collected; Usage: uses the company has for the data that is collected; Protection: striving to protect all data, howeverelectronic storage is not 100% secure; Storage: unclear location of where the content is stored
Policy does not differentiate essential and non-essential data collection	Questionable whether this information is needed for main functionality, functionality: is this information necessary given the goal of the service; Functionality: reasons for collecting personal data
Data sharing: unclear privacy implications for end-users	Users' responsibility to review third parties' privacy policy; Third: no control over the operation of third party sites; Protection: When sharing data to third parties, will ask third-party for protection

guardrails raised potential privacy compromises for people with disabilities. For example, the privacy policy for Orcam MyEye, explicitly states:

> "We reserve the right to retain any Personal Data for as long as reasonably necessary in order to: (i) fulfill the purposes described herein; (ii) in the defense or assertion of legal claims and liability; (iii) for the analyses and improvement of the Services and products; and (iv) to comply with applicable law..." (OrcamTechnologies)

We pose that the company's statement to "[retain personal data] in the defense or assertion of legal claims and liability" and "to comply with applicable law" does not reflect a policy that moves beyond legal frameworks to prioritize user privacy. That is, their emphasis on legal compliance merely institutes the minimum protections required by the law without mentioning how these laws protect users of AT. Moreover, their policy does not address the broader implications of how such treatment of user data might negatively impact the privacy needs and vulnerabilities of people with vision loss [38], the target end-users of Orcam MyEye.

We also found similar language used for the Envision App:

> "As set out under the General Data Protection Regulation, we keep personal data...for as long as is necessary...the law does not stipulate specific storage periods for personal data." (Envision Tech. B.V.)

Envision Tech. B.V.'s policy specifically emphasized adherence to the General Data Protection Regulation (GDPR)[4] but also highlighted the ambiguity in the law regarding specific storage durations. Not present in their statement, however, is a specific time frame for how long user data would be stored by the app.

We understand the need for AT companies to align their privacy policies with existing laws and regulations and acknowledge the limitations these legal frameworks might place on a company's ability to protect the privacy of its users [37]. However, the language used to describe user protection appears to favor the company over the needs of individuals with disabilities.

4.3 Policies Inconsistent When Describing Data Storage, Handling, and Security Methods

We found that how AT companies store, handle, and use end-user data differs greatly by company and is riddled with inconsistencies

[4] https://gdpr.eu/what-is-gdpr/

and a lack of transparency. While 13 AT policies delved into the nuances of data handling (e.g., fully explaining what data will be collected and specifics about how the company will use user data), 6 remained ambiguous (e.g., mentioning what user data will be collected, but only generally stating how it might be used). For example, Lazarillo's policy stated:

> "The content that you share to all users is neither private nor confidential and you should not have any expectation of privacy with respect to it. Information you upload will be posted along with other personal information" (Lazarillo, LLC.)

While the policy is straightforward about its stance on user expectations of privacy when using the AT, it falls short in detailing the nature of the "other personal information"' that might be displayed alongside user content. This omission is notable given the risk that such ambiguity could unintentionally disclose sensitive personal information [53].

In contrast, IrisVision's policy provided greater levels of detail in this regard:

> "...[We use]the collected data for various purposes...[lists services]...while we strive to use commercially acceptable means to protect your Personal Data, we cannot guarantee its absolute security...having content or information removed does not necessarily ensure complete or comprehensive removal from the Service or any other media." (IrisVision Global)

IrisVision Global's statement offers a clearer understanding of the company's data use practices by explicitly outlining the purposes for its data collection and the measures it takes to protect user data. Importantly, their policy acknowledges the limitations of securing personal data online and yet, reassures end-users of the measures taken to protect data. We propose that this transparency is a step towards empowering people with disabilities to make their own informed decisions about their data-sharing practices.

4.4 Policy Does Not Differentiate Essential and Non-essential Data Collection

Some AT policies (8 out of 18 policies) did not clearly communicate what data was essential (e.g., data crucial for the operation of the AT product) and data that was non-essential (e.g., data that is not required for the product's operation, but may add to the user experience).

For example, Dragon Voice's policy states:

> "We may collect the following sensitive data from your use of our Products...[including]... mental or physical health diagnosis, citizenship or immigration status, sex life and sexual orientation, biometric data...personal data collected from a known child, and precise geolocation data." (Nuance)

Despite communicating the types of data to be collected, it remains unclear which data is essential and non-essential to collect while using Dragon Voice. For instance, while it is conceivable that precise geolocation data might be important for certain scenarios, it is unclear why information about a user's sex life or sexual orientation would be necessary to collect.

In contrast, Lazarillo's policy states:

> "[We] may use your location and route information and/or search query history to provide navigation services and to provide information and advertisements about sites, shops and other places and attractions in your close vicinity..." (Lazarillo, LLC.)

In clarifying how a user's location and routing information might be used when received, Lazarillo, LLC.'s approach favored a more user-centric means of communicating why this information (location data) was essential to collect for the navigation service.

4.5 Data Sharing: Unclear Privacy Implications for End-Users

While some AT policies defined how data would be shared with third-party entities, there were varying degrees of transparency about the reasons for such sharing, the nature of these third parties, and the potential implications for privacy.

Sightplus' policy, for instance, stated:

> "It's hard to imagine that we would ever consider collecting, let alone sharing, sensitive information with a non-agent third party, but...we will first give you the opportunity to explicitly consent (opt-in) to such disclosure or to any use of the information..." (Vision Technologies, Ltd. (GiveVision))

Sightplus' privacy policy is explicit about how sensitive information will be treated in regard to external companies, noting that consent must first be received. We propose that this approach, through transparent data sharing, places the power of decision-making in the hands of the user.

Some AT policies appeared to shift the onus of third-party interactions onto their users, offering little to no clarity on data-sharing practices or protective measures for their information.

Supersense's policy was one such example:

> "If you click on a third-party link, you will be directed to that site. Note that these external sites are not operated by us. Therefore, we strongly advise you to review the Privacy Policy of these websites. We have no control over and assume no responsibility for the content, privacy policies, or practices of any third-party sites or services." (Mediate)

While Supersense's policy acknowledged the existence of third-party links within their platform, the company did not clarify whether third parties would have access to user data, nor did they clarify whether it would be necessary for users of their AT to share their data. This approach effectively shifts the responsibility to end-users, placing the burden on end-users to discern privacy implications when engaging with these external sites.

5 DISCUSSION

Our findings build on previous work [49, 50] to show that the limitations of existing AT privacy policies are not endemic to those designed for people with visual impairments. Most existing privacy policies lack language specific to the needs or concerns of people with disabilities. Instead, they often follow generic patterns describing data collection, use, and sharing with third parties. Furthermore, lack of transparency about third-party sharing, policy changes, and what differentiates between essential vs. non-essential data collection poses challenges to users making informed decisions about using an AT, given its privacy implications. For individuals dependent on AT that collect data over time or use services to sync their usage data, clarity on data-use practices is essential [14]. This transparency not only facilitates trust between users and AT companies by respecting user privacy but also contributes to a sense of security among users in their interactions with the technology [45].

Previous research has shown that these issues can lead to discrepancies between how experts and non-experts would interpret policies (e.g., [44]), and pose challenges in maintaining user consent in the face of policy updates and changes [18]. We challenge AT designers and privacy policy writers to look towards the broader technology industry to draw inspiration from user-centric privacy initiatives, such as Mozilla Foundation's "Privacy Not Included"[5] program, as a blueprint to tailor their privacy policies to their specific end-user population.

We further argue that the impact of these privacy policy limitations extends to personal decision-making. Disability is a universal experience, yet the experience of disability is personal and ever-changing over time [10]. This perspective on disability identity draws clear challenges to the flexibility and adaptability of AT privacy policies. Therefore, we do not propose a solution to these privacy challenges involving a one-size-fits-all approach to developing AT privacy policies. Instead, we urge AT designers and privacy policy writers to adapt their design methods in tandem with the evolving needs of their end-users, collaboratively crafting technologies and policies that empower their users to make informed decisions about AT use in a way that is aligned with their personal privacy choices.

Furthermore, policies specific to the privacy aspects of ATs can potentially motivate the development of more relevant and meaningful policies. Our analysis found that most AT policies were grounded in existing laws and regulations but did not offer tangible privacy protections beyond them. One such example is the Health Insurance Portability and Accountability Act (HIPPA)[6], which protects sensitive health information from being disclosed. However, while HIPAA provides privacy protections within a healthcare context, its limitations become evident when applied to the broader scenarios in which ATs are used. For example, the use of AT outside of the healthcare domain, such as in educational [64] and workplace [20] settings, highlights a significant gap in the protections covered by HIPPA. In other words, relying on HIPPA protections alone does not address protections in settings beyond healthcare. Therefore, we challenge AT privacy policy writers to develop a specific policy framework tailored to regulate the diverse contexts in which ATs operate.

Finally, given the growth in efforts for developing automated systems to both analyze and produce privacy policies (e.g., [48, 59]), future work can identify and operationalize AT privacy characteristics based on the real needs and concerns of end-users with disabilities to inform approaches specifically for improving the design and uptake of these emerging technologies without causing unintended privacy harms.

6 LIMITATIONS AND FUTURE WORK

We aim to address the limitations of our work with several promising future research directions:

Our data collection and subsequent analysis were limited to AT privacy policies that were publicly available on their respective company websites; therefore, we did not include privacy policies that may have been available elsewhere. Furthermore, we did not have insight into the perspective of experts developing ATs, those writing the privacy policies, AT users, or AT specialists and therapists. Understanding these experiences and perspectives would provide important insight into how end-users find, read, and interpret privacy policies. Moreover, a future interview study with security and privacy experts, especially those who develop ATs, would complement our findings on privacy policies. These experts may be able to provide additional context for why certain language was or was not included in each privacy policy, as well as clarify each company's privacy goals. They can further describe if there are other means of providing privacy information to end-users, such as tutorials, online materials (other than privacy policies), or other means. However, we observe and understand that writing informative policies is a complex and time-consuming task that many developers may not have enough resources or motivation to pursue. Future tools and guidelines for creating stronger privacy policies, preferably in collaboration with developers, can help create better policies in the future.

Additionally, even though we included privacy policies for various types of AT in our study, we did not carry out a specific comparison of these policies based on the type of AT. We believe that investigating this problem further could offer insight into how privacy is considered across various forms of AT and for different user populations. Moreover, by focusing our analysis on privacy policies of ATs available in the U.S., we acknowledge that our findings may not extend to other countries or locals due to the diversity of privacy legislation and protections globally, which could influence how privacy policies are crafted.

Lastly, given the challenges we faced in manual policy analysis, we are keen to explore the potential of automating the process. While automation is imperfect [34], it can help streamline reviewing multiple and lengthy policies [4].

ACKNOWLEDGMENTS

We thank our anonymous reviewers for their valuable time, feedback, and suggestions.

REFERENCES

[1] Idris Adjerid, Eyal Peer, and Alessandro Acquisti. 2018. Beyond the privacy paradox: Objective versus relative risk in privacy decision making. *Management Information Systems Quarterly* 42, 2 (2018), 465–488.

[2] Tousif Ahmed, Roberto Hoyle, Kay Connelly, David Crandall, and Apu Kapadia. 2015. Privacy concerns and behaviors of people with visual impairments. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. Association for Computing Machinery, 3523–3532.

[3] Taslima Akter, Tousif Ahmed, Apu Kapadia, Manohar Swaminathan, and Swami Manohar Swaminathan. 2020. Privacy Considerations of the Visually

[5] https://foundation.mozilla.org/en/privacynotincluded/about/why/

[6] https://www.cdc.gov/phlp/publications/topic/hipaa.html

Impaired with Camera Based Assistive Technologies: Misrepresentation, Impropriety, and Fairness. *International ACM SIGACCESS Conference on Computers and Accessibility* (2020), 69–74. https://doi.org/10.1145/3373625.3417003

[4] Konstantine Arkoudas, Shoshana Loeb, Ritu Chadha, Jason Chiang, and Keith Whittaker. [n.d.]. Automated Policy Analysis. In *2012 IEEE International Symposium on Policies for Distributed Systems and Networks* (2012-07). 1–8. https://doi.org/10.1109/POLICY.2012.11

[5] Farzaneh Asgharpour, Debin Liu, and L. Jean Camp. 2007. Mental Models of Security Risks. In *Financial Cryptography and Data Security (Lecture Notes in Computer Science)*, Sven Dietrich and Rachna Dhamija (Eds.). Springer, Berlin, Heidelberg, 367–377. https://doi.org/10.1007/978-3-540-77366-5_34

[6] Shiri Azenkot, Kyle Rector, Richard Ladner, and Jacob Wobbrock. 2012. PassChords: secure multi-touch authentication for blind people. In *Proceedings of the 14th international ACM SIGACCESS conference on Computers and accessibility (ASSETS '12)*. Association for Computing Machinery, New York, NY, USA, 159–166. https://doi.org/10.1145/2384916.2384945

[7] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* (2006). https://doi.org/10.1191/1478088706qp063oa

[8] Ronan T. Bree and Gerry Gallagher. [n.d.]. Using Microsoft Excel to Code and Thematically Analyse Qualitative Data: A Simple, Cost-Effective Approach. 8, 2 ([n. d.]). Issue 2. https://ojs.aishe.org/index.php/aishe-j/article/view/281

[9] David Byrne. [n.d.]. A Worked Example of Braun and Clarke's Approach to Reflexive Thematic Analysis. 56, 3 ([n. d.]), 1391–1412. https://doi.org/10.1007/s11135-021-01182-y

[10] Alarcos Cieza, Carla Sabariego, Jerome Bickenbach, and Somnath Chatterji. 2018. Rethinking Disability. *BMC Medicine* 16, 1 (Jan. 2018), 14. https://doi.org/10.1186/s12916-017-1002-6

[11] James M. Clarke, Maryam Mehrnezhad, and Ehsan Toreini. 2024. Invisible, Unreadable, and Inaudible Cookie Notices: An Evaluation of Cookie Notices for Users with Visual Impairments. *ACM Transactions on Accessible Computing* 17, 1 (March 2024), 1:1–1:39. https://doi.org/10.1145/3641281

[12] Linda Dye, Dougal Hare, and Steve Hendy. [n.d.]. Factors Impacting on the Capacity to Consent in People with Learning Disabilities. 8, 3 ([n. d.]), 11–20. https://doi.org/10.1108/13595474200300023

[13] Ram D. Gopal, Hooman Hidaji, Raymond A. Patterson, Erik Rolland, and Dmitry Zhdanov. 2018. How Much to Share with Third Parties?: User Privacy Concerns and Website Dilemmas. *Management Information Systems Quarterly* (2018). https://doi.org/10.25300/misq/2018/13839

[14] Foad Hamidi, Kellie Poneres, Aaron Massey, and Amy Hurst. 2018. Who Should Have Access to my Pointing Data? Privacy Tradeoffs of Adaptive Assistive Technologies. In *Proceedings of the 20th International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS '18)*. Association for Computing Machinery, New York, NY, USA, 203–216. https://doi.org/10.1145/3234695.3239331

[15] Foad Hamidi, Kellie Poneres, Aaron Massey, and Amy Hurst. 2020. Using a participatory activities toolkit to elicit privacy expectations of adaptive assistive technologies. In *Proceedings of the 17th International Web for All Conference (W4A '20)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3371300.3383336

[16] Foad Hamidi, Kellie Poneres, Aaron K. Massey, and Amy Hurst. 2018. Who Should Have Access to my Pointing Data?: Privacy Tradeoffs of Adaptive Assistive Technologies. *International ACM SIGACCESS Conference on Computers and Accessibility* (2018). https://doi.org/10.1145/3234695.3239331

[17] Hamza Harkous, Kassem Fawaz, R. Lebret, F. Schaub, K. Shin, and K. Aberer. 2018. Polisis: Automated Analysis and Presentation of Privacy Policies Using Deep Learning. *USENIX Security Symposium* (2018). https://doi.org/10.5555/3277203.3277243

[18] Carlos Jensen and Colin Potts. 2004. Privacy policies as decision-making tools: an evaluation of online privacy notices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '04)*. Association for Computing Machinery, New York, NY, USA, 471–478. https://doi.org/10.1145/985692.985752

[19] Desleigh de Jonge, Sylvia Rodger, and Heidi Fitzgibbon. 2001. Putting technology to work: Users' perspective on integrating assistive technology into the workplace. *Work* 16, 2 (2001), 77–89.

[20] Desleigh de Jonge, Marcia Scherer, and Sylvia Rodger. 2006. *Assistive Technology in the Workplace.* Elsevier Health Sciences. Google-Books-ID: 8gAicjzj358C.

[21] 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 *Eleventh symposium on usable privacy and security (SOUPS 2015)*. 39–52.

[22] Patrick Gage Kelley, Lucian Cesca, Joanna Bresee, and Lorrie Faith 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.* 1573–1582.

[23] Barbara Krumay and Jennifer Klar. 2020. Readability of Privacy Policies. *Database Security* (2020). https://doi.org/10.1007/978-3-030-49669-2_22

[24] Roxanne Leitão. 2018. Digital Technologies and their Role in Intimate Partner Violence. *CHI Extended Abstracts* (2018). https://doi.org/10.1145/3170427.3180305

[25] Roxanne Leitão. 2019. Technology-Facilitated Intimate Partner Abuse: a qualitative analysis of data from online domestic abuse forums. *Human-Computer Interaction* (2019). https://doi.org/10.1080/07370024.2019.1685883

[26] Heather Richter Lipford, Jason Watson, Michael Whitney, Katherine Froiland, and Robert W. Reeder. 2010. Visual vs. compact: a comparison of privacy policy interfaces. *International Conference on Human Factors in Computing Systems* (2010). https://doi.org/10.1145/1753326.1753492

[27] Lesa Lorenzen-Huber, Mary Boutain, L. Jean Camp, Kalpana Shankar, and Kay H. Connelly. 2011. Privacy, Technology, and Aging: A Proposed Framework. *Ageing International* 36, 2 (June 2011), 232–252. https://doi.org/10.1007/s12126-010-9083-y

[28] Gianclaudio Malgieri, Jędrzej Niklas, and Jędrzej Niklas. 2020. Vulnerable data subjects. *Computer Law and Security Review* (2020). https://doi.org/10.1016/j.clsr.2020.105415

[29] Martin Matzner, Jan Hendrik Betzing, Matthias Tietz, Jan vom Brocke, Brocke Jan vom, and Jörg Becker. 2019. The impact of transparency on mobile privacy decision making. *Electronic Markets* (2019). https://doi.org/10.1007/s12525-019-00332-3

[30] Aleecia M. McDonald and Lorrie Faith Cranor. 2008. The Cost of Reading Privacy Policies. (2008). https://kb.osu.edu/handle/1811/72839 Accepted: 2015-09-30T22:41:07Z Publisher: Ohio State University. Moritz College of Law.

[31] Nora McDonald and Andrea Forte. [n.d.]. Privacy and Vulnerable Populations. In *Modern Socio-Technical Perspectives on Privacy*, Bart P. Knijnenburg, Xinru Page, Pamela Wisniewski, Heather Richter Lipford, Nicholas Proferes, and Jennifer Romano (Eds.). Springer International Publishing, 337–363. https://doi.org/10.1007/978-3-030-82786-1_15

[32] Nora McDonald and Andrea Forte. 2022. Privacy and Vulnerable Populations. *Modern Socio-Technical Perspectives on Privacy* (2022). https://doi.org/10.1007/978-3-030-82786-1_15

[33] Gabriele Meiselwitz. 2013. Readability assessment of policies and procedures of social networking sites. *Interacción* (2013). https://doi.org/10.1007/978-3-642-39371-6_8

[34] Abraham Mhaidli, Selin Fidan, An Doan, Gina Herakovic, Mukund Srinath, Lee Matheson, Shomir Wilson, and Florian Schaub. [n.d.]. Researchers' Experiences in Analyzing Privacy Policies: Challenges and Opportunities. 2023, 4 ([n. d.]), 287–305. https://doi.org/10.56553/popets-2023-0111

[35] A. Mhaidli, Selin Fidan, An Doan, Gina Herakovic, Mukund Srinath, Lee Matheson, Shomir Wilson, and F. Schaub. 2023. Researchers' Experiences in Analyzing Privacy Policies: Challenges and Opportunities. *Proceedings on Privacy Enhancing Technologies* (2023). https://doi.org/10.56553/popets-2023-0111

[36] Abraham Mhaidli, Selin Fidan, An Doan, Gina Herakovic, Mukund Srinath, Lee Matheson, Shomir Wilson, and Florian Schaub. 2023. Researchers' Experiences in Analyzing Privacy Policies: Challenges and Opportunities. *Proceedings on Privacy Enhancing Technologies* 2023, 4 (Oct. 2023), 287–305. https://doi.org/10.56553/popets-2023-0111

[37] Nicolas M. Müller, Daniel Kowatsch, Pascal Debus, Donika Mirdita, and Konstantin Böttinger. [n.d.]. On GDPR Compliance of Companies' Privacy Policies. In *Text, Speech, and Dialogue* (Cham, 2019) *(Lecture Notes in Computer Science)*, Kamil Ekštein (Ed.). Springer International Publishing, 151–159. https://doi.org/10.1007/978-3-030-27947-9_13

[38] Daniela Napoli, Khadija Baig, Sana Maqsood, and Sonia Chiasson. [n.d.]. "I'm Literally Just Hoping This Will {Work:'}' Obstacles Blocking the Online Security and Privacy of Users with Visual Disabilities. 263–280. https://www.usenix.org/conference/soups2021/presentation/napoli

[39] Helen Nissenbaum. 2009. Privacy in Context: Technology, Policy, and the Integrity of Social Life. *null* (2009). https://doi.org/null

[40] Matthew J. Page, Joanne E. McKenzie, Patrick M. Bossuyt, Isabelle Boutron, Tammy C. Hoffmann, Cynthia D. Mulrow, Larissa Shamseer, Jennifer M. Tetzlaff, Elie A. Akl, Sue E. Brennan, Roger Chou, Julie Glanville, Jeremy M. Grimshaw, Asbjørn Hróbjartsson, Manoj M. Lalu, Tianjing Li, Elizabeth W. Loder, Evan Mayo-Wilson, Steve McDonald, Luke A. McGuinness, Lesley A. Stewart, James Thomas, Andrea C. Tricco, Vivian A. Welch, Penny Whiting, and David Moher. 2021. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *Systematic Reviews* 10, 1 (March 2021), 89. https://doi.org/10.1186/s13643-021-01626-4

[41] Michael Quinn Patton. [n.d.]. *Qualitative Evaluation and Research Methods* (2nd edition ed.). SAGE Publications, Inc.

[42] Stanislaw Piasecki and Jiahong Chen. [n.d.]. Complying with the GDPR When Vulnerable People Use Smart Devices. 12, 2 ([n. d.]), 113–131. https://doi.org/10.1093/idpl/ipac001

[43] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J. Aviv. 2019. "Woe is me": Examining Older Adults' Perceptions of Privacy. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, Glasgow Scotland Uk, 1–6. https://doi.org/10.1145/3290607.3312770

[44] Joel R. Reidenberg, Travis D. Breaux, Lorrie Faith Cranor, Brian French, Amanda Beth Grannis, James T. Graves, Fei Liu, Aleecia M. McDonald, Thomas B. Norton, Rohan Ramanath, N. Cameron Russell, Norman Sadeh, and Florian Schaub. 2014. Disagreeable Privacy Policies: Mismatches between Meaning

and Users' Understanding. *Berkeley Technology Law Journal* (2014). https://doi.org/10.2139/ssrn.2418297

[45] Isabel Schwaninger, Florian Güldenpfennig, Astrid Weiss, and Geraldine Fitzpatrick. 2021. What Do You Mean by Trust? Establishing Shared Meaning in Interdisciplinary Design for Assistive Technology. *International Journal of Social Robotics* 13, 8 (Dec. 2021), 1879–1897. https://doi.org/10.1007/s12369-020-00742-w

[46] Stephen Secules, Cassandra McCall, Cassandra McCall, Joel Alejandro Mejia, Chanel Beebe, Adam Stark Masters, Matilde L. Sánchez-Peña, Matilde L. Sánchez-Peña, Matilde Sanchez-Pena, and Martina Svyantek. 2021. Positionality practices and dimensions of impact on equity research: A collaborative inquiry and call to the community. *Journal of Engineering Education* (2021). https://doi.org/10.1002/jee.20377

[47] Diane L. Smith. 2008. Disability, Gender and Intimate Partner Violence: Relationships from the Behavioral Risk Factor Surveillance System. *Sexuality and Disability* (2008). https://doi.org/10.1007/s11195-007-9064-6

[48] Mukund Srinath, Shomir Wilson, Shomir Wilson, and C. Lee Giles. 2020. Privacy at Scale: Introducing the PrivaSeer Corpus of Web Privacy Policies. *arXiv: Information Retrieval* (2020). https://doi.org/10.18653/v1/2021.acl-long.532

[49] Abigale Stangl, Emma Sadjo, Pardis Emami-Naeini, Yang Wang, D. Gurari, and Leah Findlater. 2023. "Dump it, Destroy it, Send it to Data Heaven": Blind People's Expectations for Visual Privacy in Visual Assistance Technologies. *International Cross-Disciplinary Conference on Web Accessibility* (2023). https://doi.org/10.1145/3587281.3587296

[50] Abigale Stangl, Kristina Shiroma, Nathan Davis, Bo Xie, Kenneth R. Fleischmann, Leah Findlater, and Danna Gurari. 2022. Privacy Concerns for Visual Assistance Technologies. *ACM Transactions on Accessible Computing* (2022). https://doi.org/10.1145/3517384

[51] Ruoxi Sun and Minhui Xue. 2020. Quality Assessment of Online Automated Privacy Policy Generators: An Empirical Study. In *Proceedings of the 24th International Conference on Evaluation and Assessment in Software Engineering (EASE '20)*. Association for Computing Machinery, New York, NY, USA, 270–275. https://doi.org/10.1145/3383219.3383247

[52] Madiha Tabassum, Abdulmajeed Alqhatani, Marran Aldossari, and Heather Richter Lipford. 2018. Increasing User Attention with a Comic-based Policy. *International Conference on Human Factors in Computing Systems* (2018). https://doi.org/10.1145/3173574.3173774

[53] Vicenç Torra and Guillermo Navarro-Arribas. [n.d.]. Data Privacy. 4, 4 ([n. d.]), 269–280. https://doi.org/10.1002/widm.1129

[54] Lin Wan, Claudia Müller, Dave Randall, and Volker Wulf. 2016. Design of A GPS Monitoring System for Dementia Care and Its Challenges in Academia-Industry Project. *ACM Trans. Comput.-Hum. Interact.* 23, 5, Article 31 (oct 2016), 36 pages. https://doi.org/10.1145/2963095

[55] Yang Wang. 2017. The Third Wave?: Inclusive Privacy and Security. (2017). https://doi.org/10.1145/3171533.3171538

[56] Yang Wang and Charlotte Emily Price. 2022. Accessible Privacy. *Modern Socio-Technical Perspectives on Privacy* (2022). https://doi.org/10.1007/978-3-030-82786-1_13

[57] Rick Wash. 2010. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10)*. Association for Computing Machinery, New York, NY, USA, 1–16. https://doi.org/10.1145/1837110.1837125

[58] Rick Wash and Emilee Rader. 2015. Too much knowledge? security beliefs and protective behaviors among united states internet users. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security (SOUPS '15)*. USENIX Association, USA, 309–325. https://doi.org/10.5555/3235866.3235892

[59] Shomir Wilson, Florian Schaub, Aswarth Abhilash Dara, Aswarth Abhilash Dara, Frederick Liu, Sushain Cherivirala, Pedro Giovanni Leon, Mads Schaarup Andersen, Sebastian Zimmeck, Kanthashree Mysore Sathyendra, N. Cameron Russell, Thomas B. Norton, Eduard Hovy, Joel R. Reidenberg, Norman M. Sadeh, Norman M. Sadeh, and Norman Sadeh. 2016. The Creation and Analysis of a Website Privacy Policy Corpus. *Annual Meeting of the Association for Computational Linguistics* (2016). https://doi.org/10.18653/v1/p16-1126

[60] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019. Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300428

[61] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart Homes. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (Nov. 2019), 59:1–59:24. https://doi.org/10.1145/3359161

[62] Razieh Nokhbeh Zaeem, Rachel L. German, and K. Suzanne Barber. 2018. PrivacyCheck: Automatic Summarization of Privacy Policies Using Data Mining. *ACM Transactions on Internet Technology* (2018). https://doi.org/10.1145/3127519

[63] Sebastian Zimmeck, Ziqi Wang, Lieyong Zou, Roger Iyengar, Bin Liu, Florian Schaub, Shomir Wilson, Norman Sadeh, Steven Bellovin, and Joel Reidenberg. 2016. Automated analysis of privacy requirements for mobile apps. In *2016 AAAI Fall Symposium Series*. https://doi.org/10.14722/ndss.2017.23034

[64] Ingvil Øien, Bjørg Fallang, and Sigrid Østensjø. 2016. Everyday use of assistive technology devices in school settings. *Disability and Rehabilitation: Assistive Technology* 11, 8 (Nov. 2016), 630–635. https://doi.org/10.3109/17483107.2014.1001449 Publisher: Taylor & Francis _eprint: https://doi.org/10.3109/17483107.2014.1001449.