Privacy Concerns for Visual Assistance Technologies

ABIGALE STANGL, University of Washington
KRISTINA SHIROMA, University of Texas at Austin
NATHAN DAVIS, University of Texas at Austin
BO XIE, University of Texas at Austin
KENNETH R. FLEISCHMANN, University of Texas at Austin
LEAH FINDLATER, University of Washington
DANNA GURARI, University of Colorado Boulder

People who are blind share their images and videos with companies that provide **visual assistance technologies (VATs)** to gain access to information about their surroundings. A challenge is that people who are blind cannot independently validate the content of the images and videos before they share them, and their visual data commonly contains private content. We examine privacy concerns for blind people who share personal visual data with VAT companies that provide descriptions authored by humans or **artifcial intelligence (AI)**. We frst interviewed 18 people who are blind about their perceptions of privacy when using both types of VATs. Then we asked the participants to rate 21 types of image content according to their level of privacy concern if the information was shared knowingly versus unknowingly with human- or AI-powered VATs. Finally, we analyzed what information VAT companies communicate to users about their collection and processing of users' personal visual data through their privacy policies. Our fndings have implications for the development of VATs that safeguard blind users' visual privacy, and our methods may be useful for other camera-based technology companies and their users.

CCS Concepts: • **Human-centered computing → Empirical studies in accessibility;**

Additional Key Words and Phrases: Visual assistance technology, image description, visual question answering, remote sighted assistance, artificial intelligence, private visual content, visual personal data, privacy, privacy policy analysis, data regulation, camera-based devices, blind, visually impaired

ACM Reference format:
Abigale Stangl, Kristina Shiroma, Nathan Davis, Bo Xie, Kenneth R. Fleischmann, Leah Findlater, and Danna Gurari. 2022. Privacy Concerns for Visual Assistance Technologies. *ACM Trans. Access. Comput.* 15, 2, Article 15 (May 2022), 43 pages.
https://doi.org/10.1145/3517384

This work was supported by the University of Texas at Austin Good Systems Grand Challenge, the National Science Foundation/Computing Research Association 2020 Computing Innovation Fellows program, the University of Washington Center for Research and Education on Accessible Technology and Experiences (CREATE), and the National Science Foundation (SaTC-2126314).
Authors' addresses: A. Stangl and L. Findlater, 3960 Benton Lane NE 428 Sieg Building University of Washington Seattle, WA 98195; emails: {astangl, leahkf}@uw.edu; K. Shiroma, N. Davis, B. Xie, and K. R. Fleischmann, University of Texas at Austin, 1616 Guadalupe St, Suite 5.202, Austin, Texas, 78701; emails: {kristinashiroma, nathandavis, boxie}@utexas.edu, kfeisch@ischool.utexas.edu; D. Gurari, University of Colorado Boulder, 1111 Engineering Dr, Boulder, Boulder, Colorado, 80309.

1936-7228/2022/05-ART15
https://doi.org/10.1145/3517384

1 INTRODUCTION

People who are blind take and share images and videos of their surroundings to receive visual assistance. ***Visual assistance technologies (VATs)*** return a description of the visual content in response to submitted images or videos. VATs are supported on a variety of devices, including mobile phones [15, 34, 74, 83, 99] and smart glasses [7, 78]. VATs provide visual assistance using remote human visual assistants (human-powered VATs), **artificial intelligence (AI)** algorithms (AI-powered VATs), or a combination of the two.

Images and videos shared with VATs can contain private information [8, 45, 64, 90], which we refer to as ***private visual content (PVC)***. For example, Gurari et al. (2019) found that over 10% of the images blind people took (from over 40,000 images) show personal information such as medical, financial, computer/account login information, and faces of other people [45]. Privacy is of great concern at a time when many companies record users' personal data,[1] and even more so given that blind people cannot always know if they leak PVC to VATs prior to receiving visual assistance.

Complementing prior work in accessible computing [4, 5, 9], we examine visual privacy in the context of VATs. Through two studies, our work offers novel insight about blind people's privacy concerns when using VATs. Study 1 addresses three **research questions (RQs)** through semi-structured interviews with 18 blind participants. RQ1 was *What factors do people who are blind identify as impacting their privacy in the context of their use of VATs?* In addition to interview questions that addressed RQ1, we asked participants to complete a *Privacy Concerns Rating Task* by rating their level of privacy concern for 21 types of PVC—originally identified by Gurari et al. [45]—according to the following hypothetical but realistic *contextual conditions*: personal visual data containing PVC was leaked publicly, or it was shared *knowingly* or *unknowingly* with either *human-powered* or *AI-powered VATs*. This data enabled us to examine, *Which PVC types are of most concern to people who are blind, generally as well as when using human-powered vs. AI-powered VATs?* (RQ2), and *How does the intentionality (knowingly or unknowingly) of privacy disclosures affect what is considered to be private visual content when using VATs* (RQ3). To complement Study 1 and further understand *What VAT companies communicate to users about the collection and processing of their visual data, as embodied through privacy policies* (RQ4), we then conducted Study 2. We analyzed 13 VATs' privacy policies according to eight prompts related to the collection and processing of users' images and videos.

From the Study 1 interviews, we found that blind people's privacy perceptions are influenced by factors that fall under three themes: (1) users' own and other people's well-being, (2) their understanding of how VATs provide assistance, and (3) their underlying values. Some of these factors increase privacy *risk* while others reduce it. We present these findings for both human-powered and AI-powered VATs in Section 3. We then present findings from the Privacy Concerns Rating Task in Section 4, which provide new insights on the types of PVC that are of most concern to blind people when sharing images with human-powered vs. AI-powered VATs, and according to their awareness of the PVC disclosure. Finally, in Section 5 we present findings from Study 2 that reveal that 7 of the 13 VAT companies in our sample do not provide notice about the collection of personal *visual* data. Moreover, none of the companies provided notice about the retention of visual data, nor did they communicate to users about their choices to delete visual data or opt out of it being recorded. Only two companies mentioned whether they use visual data to develop AI, and only two companies mentioned whether they sell visual data to third parties—both do.

[1]Personal data is *"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" [80].*

We initially presented Study 1 at ASSETS 2020 [96]. This journal paper extends that work with an analysis of the Privacy Concerns Rating Task data from that study in two important ways (Section 4). First, we investigated another contextual factor that may impact VAT users' privacy concerns: the impact of one's visual experience, that is, being blind since birth (no prior visual experience) vs. acquiring blindness (prior visual experience). To do so, we conducted an exploratory quantitative comparison of the privacy concern rating scores for human-powered and AI-powered VATs according to the onset of one's visual impairment. Second, we performed a thematic analysis [22] of the short-answer responses participants provided as rationale for ratings of the 21 PVC types, and related contextual conditions. Study 2 (Section 5) is entirely new.

Together, our extended findings from Study 1 and Study 2: (1) reveal an expanded list of factors that influence VAT users' privacy concerns, (2) provide concrete guidance about the influence of different contextual conditions on users' privacy concerns overall and for each PVC type, and (3) surface a misalignment between users' understanding and desire to know how VATs handle their *personal visual data*, and what information is communicated to them within VAT companies' privacy policies. We discuss how our work may be used to develop privacy-protective human-powered and AI-powered VATs that address users' privacy concerns. Our work serves as a foundation for the development of VATs that offer human-centered privacy safeguards to *"protect people who fall outside of the 'norms' reflected and constructed by AI systems"* [54] and to develop camera-based technologies and AI systems based on ethical considerations [75, 102].

2 BACKGROUND AND RELATED WORK

In this section, we first provide background information on VATs. We then discuss our current understanding on how people who are blind use VATs, including their privacy concerns and prior efforts to develop taxonomies that indicate what content is private.

2.1 Visual Assistance Technologies (VATs)

Over the past decade, a variety of ***visual assistance technologies* (VATs)** have been developed to provide users with descriptions of their visual surroundings. There are two common types. The first type entails captioning, by taking visual content as input and returning a description of the content such as about colors, text, money, objects, and people [6, 24, 34, 55, 60, 61, 69, 74, 99]. The second type entails visual question answering, and takes both visual content and a question about the visual content as input and then returns an answer [7, 15, 18]. In this paper, we focus on VATs of both types that center on users submitting their own visual content.

VATs can be human-powered or AI-powered. *Human-powered VATs* [17] rely on humans, including crowd workers [110], friends [19], social microvolunteers [20], or trained professionals [7]. *AI-powered VATs* instead rely on AI. Prior work has shown that the privacy concerns of blind people vary when obtaining descriptions from different types of visual assistants, specifically human-powered versus AI-powered VATs [9].[2] To our knowledge, our work is the first to decipher the factors that influence the visual privacy concerns of people who are blind when using human-powered or AI-powered VATs, and the degree to which their concerns differ based on who is providing the assistance (humans versus AI).

2.2 Blind People's Use of VATs and Privacy Concerns

Prior work has studied VAT usage, including the types of images and questions blind people share with VATs [19, 25, 44, 46, 47], what information blind people want in image descriptions [40–43, 95],

[2]While Li et al. [66] offer a comprehensive overview of the variety of data recipients considered in prior works at the intersection of privacy studies and human-computer interaction, they do not include specialized technologies like VATs as recipients.

ethical considerations regarding AI [13], user-centered evaluations of the accuracy of AI-powered visual descriptions [70], as well as how remote sighted assistants provide visual assistance [64, 90].

Most related to our work is that which focuses on the privacy, security, and safety concerns of blind people when using camera-based technologies [3–5, 12, 21, 51, 58, 63, 89], and in particular camera-based technologies that provide visual assistance [8, 9]. In a survey study with 155 people who are blind or have low vision, Akter et al. [9] found that participants' concerns about VATs and privacy shifted according to (1) who received their data and their relationship to that person/service as well as (2) whether or not they share images showing themselves versus images showing other content. In a subsequent study, Akter et al. [8] identified the privacy implications when blind people capture bystanders in their images (where their faces were revealed).

In contrast to the above work, our paper provides concrete guidance regarding the types of personal visual data blind people perceive to be private in the context of VAT use. Whereas Akter et al. [9] examined five types of PVC, we analyze 21 privacy types. Second, we study how people's privacy concerns change according to the contextual conditions in which they may share their private data, i.e. *knowingly* versus *unknowingly*, given that blind people both intentionally and inadvertently share information they consider to be private with VATs [1, 45, 56].

2.3 Visual Privacy and Privacy Taxonomies

Taxonomies to define private visual content have emerged from the AI community, where the focus has been on automating the task of recognizing PVC. These taxonomies offer guidance regarding *what type* of visual content is private [38, 46, 66, 79, 109]. Others have created taxonomies to assess *how* private an image is (e.g., to be shared only with the family, friends, or everyone) [2, 14, 93]. Our work draws on the work of Gurari et al. [45], who conducted a visual analysis of approximately 40,000 images taken and shared by blind people with a VAT deployed in 2011 called VizWiz [18]. Their analysis resulted in a taxonomy of 19 types of PVC, organized according to two parent categories, Private Objects and Private Text, and provides a foundation for the development of AI algorithms that can identify PVC in images taken by blind people. In this paper, we extend [45] by asking blind people to independently identify the types of image content they consider to be PVC, and rate their level of privacy concern if they shared each type of PVC identified in [45], under the contextual conditions: *knowingly* or *unknowingly* with human-powered or AI-powered VATs, or publicly. Our human-centered approach helps to bridge the gap between research on AI privacy and privacy considerations related to accessibility.

2.4 Privacy Policy Analysis

Privacy policies are the primary mechanism through which companies communicate to users their data collection and processing practices. The ***Fair Information Practice Principles (FIPPs)*** [27] of 1980 established the precedence for the establishment of both sectoral data regulations[3] in the United States and the omnibus data and privacy regulations in Europe, e.g., **General Data Protection Regulation (GDPR)** [33]. Data regulations describe policies and laws ensuring that collected and processed data is shared or governed appropriately, where the right data assets go to the right place at the right time. Data regulation falls under the umbrella of Data Governance.

FIPPs also established the precedent of *"Notice and Choice"*, the aim of which is to put individual users in charge of the collection and use of their personal information [85]. "Notice" entails that

[3]Examples include Children's Online Privacy Protection Act of 1998 (COPPA) [28], Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act [29], Gramm-Leach-Bliley Act [30], California Consumer Privacy Act (CCPA) [77], and Health Insurance Portability and Accountability Act (HIPAA) [101].

companies provide a legal document outlining their data handling practices—collection, retention, use, and selling of personal data. "Choice" gives consumers options as to how any personal information recorded from them may be used [26]. Despite mounting criticism of the effectiveness of "Notice and Choice" for users (referred to in data regulation as "data subjects"), e.g., [84, 104], privacy policies are still the primary mechanism for a company to inform users about the collection and processing of personal data [67]. In Study 2 of this paper, we present an analysis of 13 major VAT companies' privacy policies using the "Notice and Choice" framework.

Privacy policy analysis has been widely used to evaluate if companies adhere to data regulation and to assess their effectiveness in informing users about data collection and processing practices [23, 48, 57, 84, 86, 91]. Prior work has shown that privacy policies are often difficult for users to comprehend due to language complexity and inconsistent policy format [59, 62, 73, 87], and the time required to read them [71]. In turn, researchers have thus sought to develop strategies to improve privacy policy accessibility [59, 65, 68, 82, 98, 100, 103, 112], and have created tools to aid users in reading and interpreting the policies themselves [50, 62, 82, 94, 106, 108, 111]. Our work, however, most closely relates to analyses of what content privacy policies communicate, e.g., [48, 52]. For instance, Habib et al. [48] found that choices are often not adequately described for email marketing, targeted advertising, and data deletion. To our knowledge, we are the first to investigate what VAT companies communicate to users about what happens to *personal visual data* (e.g., images and videos) through privacy policies.

3 SEMI-STRUCTURED INTERVIEWS WITH BLIND PEOPLE

We now present our research that is guided by RQ1: *What factors do people who are blind identify as impacting their privacy in the context of their use of VATs?*, which we addressed through semi-structured interviews with 18 participants. The research presented in this section was originally published in Stangl et al. [2020] [96].

3.1 Methods

3.1.1 Participant Recruitment. We recruited participants by circulating an IRB-approved announcement on social media, on a listserv managed by organizations serving people who are blind or have visual impairments, and through snowball sampling. To be eligible, participants had to be 18 years or older, blind, and use cameras to collect and share visual media. We aimed to have equal distribution of participants in terms of gender and level of prior visual experience (i.e., born blind versus acquired blindness). We compensated participants with Amazon gift cards ($20/hour).

We interviewed 18 participants (11 female/7 male, ages 22-73 years with an average age of 42). All were located in the United States or Canada and identified as being totally blind. Nine of them were blind from birth, and nine had acquired blindness. Two of those with acquired blindness lost their sight as teenagers, three lost their sight in their 20's, and one in their late 40's. The participants' level of education varied: eight participants had completed high school, four had a bachelors degree, four had a masters degree, and two had a higher degree (e.g., JD or PhD).

3.1.2 Semi-Structured Interview Protocol. Two researchers conducted all interviews over the phone during Spring 2020. One researcher led the interviews while the other took structured notes. All interviews were audio recorded and lasted from 1-2 hours, covering the semi-structured interview questions (discussed in this section) and a privacy concern rating task (to be discussed in Section 4) . The 21 semi-structured questions focused on participants' use and preferences for different VATs, their understanding and reactions to how the services work, the types of visual

content they consider to be private, and their definitions of "privacy" and "privacy concerns"[4] outside the premise of VATs. This was important in establishing what privacy concerns naturally emerged and the role VATs play in the life of each participant prior to introducing them to the pre-established list of PVC. Similarly, we asked participants about what image and video content they self-identified as private before exposing them to the predefined PVC types during the Privacy Concern Rating Task. We designed the semi-structured interview to take approximately 45 minutes.

3.1.3 Data Analysis. We analyzed the interview data through thematic analysis [22]. We began by writing analytic memos after each interview to support our reflection and to identify emergent patterns, categories, and concepts [97]. For the first three interviews, two researchers transcribed the interviews, wrote analytical memos, then together compared their memos and resolved any disagreements through iterative discussion. For the subsequent 15 interviews, the two researchers took turns transcribing and writing memos. After each memo was complete, the second researcher reviewed the first researcher's memo.

After all interviews were complete, we used affinity diagramming [16] to collaboratively identify an initial set of themes that were present across the analytic memos. We drew on these themes when analysing the interview transcripts. Two researchers reviewed each interview transcript, selected and labeled instances where participants reflected about privacy when using VATs, and occasionally refined the theme names and re-coded segments under a different theme. We also applied codes to the segments of interview text when the participants referenced human-powered or AI-powered VATs in their statements, and if their reflections conveyed a risk or benefit to their sense of privacy. Finally, we categorized the themes (factors) according to three broader categories that first became apparent when reviewing the analytic memos:

(1) *Understanding of the Service Offering:* Instances when participants reflected on or shared their understanding of how the VATs deliver their services; this covered both their sense that privacy is at risk and their sense that their privacy is bolstered by VATs;
(2) *Personal/Social Impact:* Instances when participants made statements about the VATs and how their service offerings either add a risk or a benefit to their personal or their communities' sense of well-being;
(3) *Values-Based Assessment:* Instances when participants made statements that defined or exemplified a set of beliefs or morals related to their privacy in the context of their human-powered and AI-powered VAT use.[5]

3.2 Results

In this section, we first summarize participants' VAT use. We then present other interview findings, including: (1) participants' definitions of privacy, (2) the factors that impact their sense of privacy when using human-powered and AI-powered VATs, and (3) the types of image content participants identified as PVC.

[4]Concerns consist of feelings, preoccupations, thoughts, and considerations [49]. We chose to interview participants about their concerns, as opposed to engaging them in a contextual inquiry, based on our understanding that investigation of attitudinal factors should precede behavioral studies [81, 92].

[5]Human values can be understood as *"what a person or group of people consider important in life"* [37]. Thus, values intermediate between individuals and groups, as they are held by and shared among individuals within a group. Values are formed fairly early in life, and are trans-situational, meaning that values guide behavior at a level above attitudes, which depend on specific situations, people, or objects [88]. Values are critical for understanding how individuals interact with information [35].

Table 1. The VATs Most Commonly Used by the Participants in Our Study and the Tasks They Use the VATs to Accomplish

VAT	Users	Use-Case Across All VATs	Use-Case Specific to Each VAT	Frequency of Use	Duration per Session
Aira	10	Reading mail, food packaging and recipes, appliance displays, and street signs	Reading documents with social security numbers or credit card numbers; cooking; navigating websites; signing documents; taking photos; looking for jobs; and obtaining descriptions of videos and pictures.	Once a month to 7 days per week	5 to 90 minutes
Be My Eyes	4		Reading objects with curved surfaces; locating lost items; fixing broken objects.	1 to 3 times per week	5 to 10 minutes
Seeing AI	4		Reading text on medication bottles and in images; scanning bar codes; image descriptions; and restringing a guitar.	2 to 5 times per week	2 to 10 minutes

3.2.1 Use of VATs. All participants had experience with both human-powered VATs (Aira and/or Be My Eyes) and AI-powered VATs (Seeing AI and/or Envision AI) on iPhones. However, when asked which VAT they use the most and for what purposes, 10 participants reported their primary VAT to be Aira, four reported Be My Eyes, and four reported Seeing AI. Table 1 shows what tasks participants accomplish with each VAT, and the frequency and duration of use.

While participants reported using VATs for reading text in mail, documents, and food packaging, we also observed that some tasks were unique to specific VATs. For example, participants used Aira to interact with live human visual assistants and to complete tasks such as signing documents, selling on eBay, resolving issues on productivity applications, and reading credit cards and documents with social security numbers. Moreover, one participant explained how an Aira agent provided them with assistance to search for and complete a job application (a task that took 90 minutes on a paid account).

The participants who prefer to use Be My Eyes, a VAT that utilizes volunteers to provide visual assistance, highlighted the value they experience when being able to interact with a human assistant that could be located anywhere in the world. The participants use Be My Eyes to fix broken objects, obtain support using productivity applications, find lost items, and read text on objects with curved surfaces—a task that one participant stated was *"too hard for AI"*. The four participants who preferred Be My Eyes reported using it for five to ten minutes per session.

Those who preferred using Seeing AI indicated that they use it because it is the *"most efficient"* VAT and that they could accomplish their tasks between two to five minutes, two to five times a week. They use Seeing AI for its variety of features—from the short text reader, object identifier, and barcode reader. These features are useful for reading text in images, learning about the objects in an image, scanning barcodes, and completing tasks like restringing a guitar. Though our data may not comprehensively represent possible uses for VATs, these responses are consistent with prior work (e.g., [19, 46]).

3.2.2 Defining Privacy in the Context of VATs. We asked participants to describe what 'privacy' meant to them in the context of VATs. Participants described privacy in several different ways—as an experience or as related to one's behavior. For example, several participants focused on privacy being a safeguard. Regarding experience, P16 noted, *"So much stuff going on in the world, there needs to be something so people can have a sense a peace, and not isolate or hideout just to protect themselves."* Others spoke about privacy in terms of maintaining a sense of control or ownership

of information. P07 said, *"Privacy means personal control over information that was not necessarily intended for a wide distributed audience."* Regarding their own behavior of personal management, P08 said, *"I need to know who has access to my information and where it's being stored. I make sure I'm dressed, pay attention to surroundings. Try to use my headphones...I can regulate upfront."*

Others discussed privacy in terms of negative impacts from the loss of privacy: loss of control or the ability to manage what information they share, loss of ownership, loss of peace of mind. In the words of P18, *"I am concerned about privacy when my personal life is being intruded on...what I read, what I say online, what meal I ate, who I talk to, where I go. These are all mine."* P05 shared, *"Privacy concern [means] that someone takes sensitive information and the use has consequences for me."* Others focused on malicious acts, including P17 who identified *"A breach of my personal information...[use by] someone who will go to the effort to delete their tracks"* and P03 who said, *"Pertinent information that you don't want anyone else to use involuntarily [without your consent] or use to harm you in some type of way"*.

Finally, throughout the interviews participants directly identified their blindness as a factor that increases their need for privacy protections. For example, P04 shared, *"I recognize blind people have less [privacy] because we stand out in a crowd. I don't like it, but I just have to accept that"*, and P08 explained, *"After interacting with other blind people [in my daily life], I sometimes forget that when interacting with sighted people that I might need to take precautions. I can regulate up front, but it's hard to know what is out there. My identity is on the line and I need protection too."*

3.2.3 Factors Impacting Users' Visual Privacy Perceptions. During the interviews the participants shared their perspectives about what causes visual privacy *risks* and what provides a sense of visual privacy, i.e. what *benefits* their sense of privacy in the context of human-powered and AI-powered VAT use (RQ2). Below we share the *factors* the participants attributed as privacy risks and benefits for both VAT types, which fall under three overarching categories: (1) their understanding of how VATs provide the services, (2) their perceptions of the impact of sharing PVC to their personal well-being or social relationships, and (3) their assessments of how VAT services adhere to their values or raise values-based questions.

Human-powered VAT- Benefits:

Understanding of the Service Offering: Several factors related to participants' understanding of how VATs provide their services. First, we heard a belief or assumption that human-powered VATs enact practices to maintain professional standing within industry or with their users *(professionalism)*. For instance, P06 stated, *"I just assume they are a company that wants clients. Why would they sell your info?"* P05 echoed a similar sentiment, *"The company reputation would be on the line if word got out they were stealing data."* Several participants indicated that their understanding and trust in the professionalism of the service was due to the human-powered VATs' corporate messaging. For instance, P06 shared that she had received emails from Aira, which provided her with a sense of trust in the services.

Several participants noted that they perceived human-powered VATs to be professional and trustworthy due to internal and public-facing policies designed to protect users. One policy identified as beneficial was the *choice to opt out* or not to share personal visual data with the human-powered VAT. For example, P11 said, *"With Aira, you can opt out of having your info retained! It's a nice notion, but I forget about it when I'm actually using the service."* Another policy that participants brought up in the context of Aira related to the companies mandates for its employed agents (sometimes referred to as remote sighted assistants [64]) to *self-identify* at the beginning of a call. P05 noted, *"With Aira, agents identify themselves. I don't get a full [name], but at least I have a name and a time with my call log if I have to report."* P05 went on to relate the VATs service offerings to other assistive company policies, *"Aira is track-able, similar to knowing who your Uber driver is."*

Participants explicitly noted that interacting with *trained agents* is of great benefit to their sense of privacy because of the specialized training employees receive to handle PVC. For instance, P05 shared, *"When I have to get my CC info read, I'd rather do Aira because the service has trained agents and I know where to go back to if I have a problem. I check my statements and they match. They've signed whatever they have to contractually, for accountability, whereas with some of the volunteers you wouldn't have that."* Similarly, P09 expressed, *"Part of the reason [I] use Aira is because I feel like it's a company and they [Aira agents] have training. Someone could be fired, blackballed. There's a little more implicit trust."*

Values-Based Assessment: Some participants mentioned factors related to values when describing what they consider to be important when using human-powered VAT and/or how the VATs they use uphold or represent their values. Most prominently, we heard statements like *"If a human being is doing something, the assumption is they are doing their best. They are trying to do a good job, which is the vast majority of the time"* (P02). Participants' *trust in human decency* or belief in the inherent good or benevolence of remote sighted assistants reflects why blind people *knowingly* share their PVC. When discussing the benefit of Be My Eyes [34], a volunteer-based human-powered VAT, P16 expressed, *"Volunteers haven't given me a reason to not trust them."* In fact, for some participants, the opportunity to interact with volunteers from all over the world increased their trust in human decency and in some cases was *"a source of joy"*. Participants' also extended a sense of trust from the remote sighted assistants to the companies. For example, P15 said, *"From what I've heard, Aira is the best way to go. They're really trustworthy and they won't pick on you for a high balance."* During the interviews we also learned that some participants use volunteer-based human-powered VATs such as Be My Eyes because these services preserve their *anonymity* when sharing private visual data. As P07 explained, *"The benefit is [that] the anonymous [Be My Eyes volunteers] people...don't have connections to the blind community."* This participant explained that Be My Eyes alleviates the social stigma he encounters when family or friends access his images containing PVC.

Human-powered VAT- Risks:

Understanding of the Service Offering: Many participants reported a lack of understanding on VAT companies' data retention practices, which we coded as *unknown data handling*. For instance, P05 explained, *"Well, anytime you have to get something read, are they going to remember it, store it?"* They went on to discuss her specific concern with storage of information, *"I know Aira stores info, but don't know what triggers [data] retrieval or if they do. I think I saw someone say on social media that it's 18 months storage, but I haven't verified that."* P08 shared specifically about data retention, *"I don't think any [of] them [VATs] try to do that?"*

Personal/Social Impact: A risk that participants associated with human-powered VATs is *identity theft*. Participants expressed concerns that human-powered VATs created opportunities for nefarious actors to access their PVC and illegally use the information for personal gain. Put simply, P10 specifically mentioned identity theft as a privacy concern because they are *"Not comfortable with another person reading my information."* Similarly, P18 talked about having trouble setting up an online account and the sensitive information they were concerned about disclosing, *"I recently tried to set up an account on the Social Security administration website and I couldn't, I couldn't figure it out. It kept kicking me out ...when trying to set up the login. I'm sorry, I just do not feel comfortable calling up Aira or Be My Eyes, and saying can you help me create my login for Social Security."*

Some participants expressed a *fear of social judgement* related to their use of human-powered VATs, including that disclosure of PVC could solicit a negative critique from others, causing personal embarrassment or other negative psychological impact. P17 explained, *"There's certain things I may not want a human actually reading to me, that might be embarrassing, might be too personal,*

might be beyond the jar of mayonnaise, you know." Others shared the concern that when using human-powered VATs they were at higher risk for not acting in a socially acceptable manner *(not socially acceptable)*. P06 shared this fear in terms of violating another person's comfort, *"I wouldn't ask Aira to describe a [picture of a private body part]. It's inappropriate because you're disturbing someone."*

Values-based Assessment: Some participants indicated that they were at greater risk when using VATs that involve volunteers as remote sighted assistants because they lack *accountability*. For example, in the context of Be My Eyes, P09 explained, *"If someone isn't being paid, who knows what mysterious ways they are looking to gain from the system. When someone is being paid there's a lot less to think about things in that way because to them it's a job and they have some amount of job security provided they don't screw up too badly. They are too busy making sure they keep their job."* P05 shared a similar statement on the nature of volunteer-based human-powered VATs: *"I haven't used the volunteer one because you never know what you're going to get in terms of quality of the volunteer."*

AI-powered VAT- Benefits:

Understanding of the Service Offering: Some participants specified that using AI-powered VATs ensures that there are *no human eyes on data*, such as a person looking at the image or having access to the image. To this point, P10 said, *"I still feel like I have more privacy with Seeing AI, [because there is] not another human on the other end... I don't have to worry about someone writing down my information and taking it."* She later said, *"I have more trust with AI"* and though *"It [VAT] stores or can store information, it just moves on"*. Similarly, P04 indicated she trusts that AI-powered VATs do not focus on or identify an individual, thus ensuring anonymity: *"I don't mind if my data is used in the aggregate."* P13 said, *"I'm more likely to use Seeing AI. It's not necessarily more efficient, but I can plug headphones in and read it and I don't have to worry about anyone remembering my information or jotting down numbers."* In such statements, we heard participants indicate a benefit of using AI-powered VATs is that their personal visual data is not collected and/or retained by a person (e.g., P13's case) or by the service itself. P12 explained: *"I don't think of privacy because it's happening while I'm doing it. It's not being saved that I can tell."*

Personal/Social Impact: Several study participants indicated that a benefit of AI-powered VATs was that they eliminate the risk or sustained *fear of social judgement* (which occurs when using human-powered VATs). For instance, P08 stated AI-powered VATs are *"Easier and faster and I don't have someone making a judgement."* P08 went on to explain her belief that people make judgements of others, even during assistance, therefore she values AI-powered services. Accordingly, the primary benefit we heard from participants about AI-powered VATs related to privacy is that these services eliminate the possibility of embarrassment or other psychological impact.

Values-based Assessments: Similar to human-powered VATs, participants indicated that AI-powered VATs offer a sense of *anonymity* and in turn a sense of assurance that their PVC will not be linked back to them. Yet, we often heard participants state that AI-powered VATs offer more anonymity than human-powered VATs. P11 stated he values anonymity provided by AI-powered VATs, *"for speed efficiency and a little more anonymity."*

AI-powered VAT- Risks:

Understanding of the Service Offering: Often, participants discussed their lack of understanding of how AI-powered VATs handle personal visual data once collected or the service's promised privacy protections *(unknown data handling)*. P02 rhetorically asked, *"What happens to the picture after it runs through the database?"* Similarly, P04 faced her own lack of understanding, *"I never thought to ask until now, but with the AI it makes me wonder if records are kept, who keeps*

the photographs. Are they kept in the cloud somewhere or are they just kept on my phone?" More optimistically, P08 stated her concern: *"Privacy is similar because I don't know either service...both have the same access of a file to keep, replicate, or share outside"* and then followed up with *"I don't think any of them try to do that."* Later in the interview, P08 expressed further concerns, *"I don't like reading some of my mail because now it's in my phone and I don't know how it makes it to the cloud."* In response to using Seeing AI, P01 said, *"I don't understand as much as far as where the information goes, I don't know."*

Some participants had a more nuanced understanding of the VATs' policies and raised questions about the length of data retention. Regarding Seeing AI, P05 stated, *"I just don't know how long they store information"*. It was evident that participants were concerned about how VATs handle their data, and indicated that the lack of transparency creates a lack of trust. P05 went on to discuss his concern, *"I don't know how long they store it [my data]. It's a concern, but I hope that people are generating so much data they aren't tracking mine."* Others raised concerns that the AI-powered VAT *systems are vulnerable*, or in the words of P01, *"In the wrong hands someone can do anything with your information."* Some participants raised the explicit concern that their PVC could be exposed by faulty technology, without clarifying how this could arise.

3.2.4 Self-Identified Private Visual Content. Throughout the semi-structured interview we learned about the types of information the participant's self-identified as PVC. Here we report on these PVC types, and compare them to the PVC types Gurari et al. [45] identified (through a visual analysis of images taken and shared by blind people with the VizWiz [18]),which we used in the Visual Privacy Concern Rating Task presented in Section 4.

The PVC types that both the participants in our study and Gurari et al. [45] include are: *Financial Account Information* (credit card, credit report, PIN number, point of sale, financial data, "financial stuff", debit card information, financial, purchases, and banking information); *Medical Information* (health data, "health stuff", medical records, "medical stuff", pregnancy test, and Medicaid); *Identification and Location Information* (personal information, ID information, address information, name, phone number, and ID cards); *Paperwork*, (mail, personal mail, and documents); *Computer/Online Access* (login information, password, browsing history, and emails); and *People* (pictures of faces).

Our findings also revealed types of PVC that were not presented in Gurari et al. [45]. Most prominently, eight participants spoke about *Social Security Information*. For instance, P18 explained that blind people commonly use social security information to apply for Supplemental Security Income (SSI) benefits. Two participants (P02, P13) indicated they consider *Information from an Educational Institution* (such as transcripts and disciplinary reports) as PVC because disclosure of this information to the wrong parties could cause embarrassment or would betray trust. While a majority of their responses were general enough to categorize, some participants offered very specific content. These responses seemed to be representative of *Personal Interests* that they considered subject to social judgment. For instance, participants indicated images that showed *"guns"* or *"sexual identity"*, would be PVC. P17's concerns included *"books I've read."* Finally, participants commonly made statements like that from P07, *"It's hard to know the whole list of things."*

3.3 Summary

In this section we described how participants define privacy and the types of image content they considered to be PVC—extending those identified in [45], and addressed RQ 1, *What factors do people who are blind identify as impacting their privacy in the context of their use of VATs?* Table 2 offers a condensed view of these factors according to whether they add benefit or risk to a person's sense of privacy when using human-powered and AI-powered VATs. This table shows that participants perceive human-powered VATs to offer privacy protections due the human assistants'

Table 2. Summary of the Primary Factors That Influence Participants' Perceptions of Privacy in the Context of Using VATs

	Benefit		Risk	
	Human-powered VATs	**AI-powered VATs**	**Human-powered VATs**	**AI-powered VATs**
Understanding of the Service Offering	**a)** Professionalism, **b)** Corporate Responsibility, **c)** Internal and Public-facing Policies	**a)** No Human Eyes on Data	**a)** Unknown Data Handling	**a)** Unknown Data Handling, **b)** Faulty Technology
Personal/Social Impact		**a)** [Eliminate fear of] Social Judgement	**a)** Identity Theft, **b)** Social Judgement	
Values-Based Assessments	**a)** Trust in Human Decency, **b)** Interaction, **c)** Trust Extends from Humans to System Design, **d)** Anonymity	**a)** Anonymity	**a)** Accountability	

Professionalism and the companies' privacy policies, whereas the strongest privacy-preserving factor for AI-powered VATs was the assumption that people never see their data, i.e., *No Human Eyes on Data*. For both types of VATs, participants were concerned that they do not fully know if or how their PVC will be collected, stored, processed, used, and sold, which we coded as *Unknown Data Handling*. This finding motivated our analysis of 13 VAT companies' privacy policies, which we present in Section 5.

4 VISUAL PRIVACY CONCERN RATING TASK

Here we address RQ2: *Which PVC types are of most concern to people who are blind, generally, as well as when using human-powered vs. AI-powered VATs?*, and RQ3: *How does the intentionality of privacy disclosures affect what they consider to be PVC when using VATs?* An abbreviated version of this research was presented at ASSETS 2020 [96]. We extend our previous findings with new analysis in Sections 4.2.3 and 4.2.2, which draw on the ranking findings to provide further insight into factors that impact blind people's privacy perceptions when using VATs (RQ1).

4.1 Methods

Following the semi-structured interview, we conducted this **private visual content (PVC)** rating task with the same 18 participants reported in Section 3.

4.1.1 Rating Task Protocol. The rating task involved 21 PVC types. To establish these PVC types we expanded Gurari et al.'s [45] 19 PVC types by adding two more general types (Name and Location) to observe them as independent PVC types (they were compounded in the original taxonomy). We chose to provide the 21 pre-identified PVC content types to ensure that the PVC types were consistent across all participants, and in anticipation that the task of self-identifying types of PVC on the spot, without context, could be challenging for participants.[6]

For each PVC type, we prompted participants with the following question: *"Imagine that [X PVC] was available for anybody to use. How would that make you feel?"* When participants expressed a

[6]We did not include the new self-identified PVC types in the rating task as they emerged during the interviews; they may be explored in future research.

Table 3. Definitions Used During the Second Part of Our Interviews

Concern Rating Index		
Concern Level		*Definition*
1	Not	Doesn't faze me.
2	Mildly	Think about it after the fact.
3	Concerned	Discuss it with other people.
4	Very	Develop strategies to change my behavior.
5	Extremely	Change my behavior immediately.
Conditions Index		
	Definition	
P	Private Visual Content (PVC) is shared with the *Public*	
HK	Private Visual Content (PVC) is shared with Human-powered VATs *Knowingly*	
HU	Private Visual Content (PVC) is shared with Human-powered VATs *Unknowingly*	
AK	Private Visual Content (PVC) is shared with AI-powered VATs *Knowingly*	
AU	Private Visual Content (PVC) is shared with AI-powered VATs *Unknowingly*	

We asked study participants to rate their level of concern (top half) with respect to five different conditions (bottom half) for each PVC type.

concern, we followed up by asking *"In what situations would it be of particular concern to you?"* These questions enabled us to learn about participants' concerns agnostic of how the data became available or the type of VATs they use and share their visual information. We asked participants to rate their level of concern by specifying a score between 1 and 5 (1 = Not Concerned/5 = Extremely Concerned) if the PVC were to be publicly shared.[7] We then asked participants to rate their level of concern according to four other conditions, shown in Table 3. These four conditions capture how people's privacy concerns change (1) if the agent providing the description was AI-powered vs. human-powered, and (2) if they share their private data *knowingly* vs. *unknowingly*. For each condition, we also asked participants to provide a short explanation of their privacy concern rating. In total, each participant provided 105 responses (i.e., 21 types × 5 conditions). We randomized the order of the PVC types for each participant interview, though presented the conditions to them in the same order as shown in Table 3.

4.1.2 Data Analysis. We: (1) averaged the 18 participants' privacy concern ratings for each of the 21 PVC types according to the five conditions (Table 3), and (2) ordered and compared the averages for each PVC type. This analysis provided a foundation to address RQ2, *Which PVC types are of most concern to people who are blind, generally as well as when using human-powered vs. AI-powered VATs?*

The rating task data also contained 1,890 short-answer justifications that participants provided for each of their rating scores (21 PVC types × 5 conditions × 18 participants). To analyze these short-answer responses, we organized the data into 21 unique spreadsheets (one for each PVC

[7]When developing this privacy concern rating scale we considered using the "Stage of Concern Scale" [49], which has been widely used to rate one's level of arousal and perceived need for resolution in response to a technology or innovation. The scale collects data about concern according to one's awareness of the issue, the information one needs about the issue, the impact the issue has on the person, what one does to manage the issue, potential perceived consequences, what is needed for collaboration around the issue, and how one would refocus or resolve the issue. While we did draw on the "Stage of Concern Scale" during data analysis and reporting, we chose not to use this scale during the interviews after testing its application to the PVC content areas with a graduate researcher who has extremely low vision. We found that the scale introduced considerations that were not relevant to one's consideration and handling of PVC, and it was overly cognitively taxing to make sense of each consideration in relation to PVC.

type) and assigned in vivo codes[8] to each response. When these in vivo codes were reflective of the factors identified during the interview data analysis, re-coded the data accordingly and refined the definitions. Otherwise, we created new codes. After consolidating the coded short-answer data into a single spreadsheet and filtering them according to each code respectively, we merged or reassigned codes for a few responses when they had the same meaning but used different terminology.

This process resulted in 54 unique codes that fit under the parent codes (Understanding of the Service Offering, Value-Based Assessments, and Personal/Social Impacts), with each one attributed as a perceived privacy risk, benefit, or other. Twenty-four of the 54 codes convey *risk* factors that participants attributed to their privacy concern ratings. All codes and definitions can be found in the Supplementary Materials.

In all, we coded 901 of the responses as risk factors, with the most frequent code (n = 115) being *Unknown Data Handling*—a participant's assessment that the person is unaware if or how VAT company accesses, collects, stores, processes, shares, or sells PVC to a third party. We thus further investigated the *Unknown Data Handling* code through two secondary analyses. First, the lead author counted the responses coded as Unknown Data Handling—across all conditions. They reevaluated whether each of the 115 responses fit under this code, identified which condition and PVC type the short-answer response and code was attributed to, and then used a spreadsheet to sort and create a representation of the data showing how it is distributed across the contextual conditions in which PVC can be shared–i.e., with human-powered or AI-powered VATs, *knowingly* or *unknowingly*. Second, we performed a thematic analysis [22] of the 115 *Unknown Data Handling* responses, and applied codes under the general categories: privacy risk, privacy benefit, and other. We report the findings of these two secondary analyses in Section 4.2.2.

Finally, we performed a three-step analysis to address an emergent hypothesis that a participant's *prior visual experience* may be another factor that impacts the person's privacy concern ratings. First, we segmented the rating data according to whether participants were born totally blind and thus had *no prior visual experience* ($N = 9$) or acquired blindness and thus had *prior visual experience* ($N = 9$) according to each of the PVC types. Next, we averaged all participants' scores for a given PVC type and for each of the four conditions (sharing PVC with human-powered VATs *knowingly* and *unknowingly*, and with AI-powered VATs *knowingly* and *unknowingly*). Finally, we compared the average privacy concern ratings from participants with congenital blindness to those with acquired blindness according to each PVC and VAT type.

4.2 Results

4.2.1 Rating Results According to PVC Type. Here we present the results from the *Privacy Concern Rating Task*, according to seven higher-level PVC clusters. Under each cluster we summarize the privacy concern scores shown in Table 4 and the participants' rationales for providing the scores. We then present the results from two secondary analysis of the rating task data, including an examination into (1) the top rationale that the participants' shared as adding a sense of risk to their visual privacy, and (2) the impact of one's *prior visual experience* on their concern score.

Financial: Reinforcing the interview findings, the participants rated Financial Account Information as the most concerning of the 21 predefined PVC types. We examine this finding based on the context in which the content is shared (Table 3):

[8]In vivo coding is the practice of assigning a label to a section of data, such as an interview transcript, using a word or short phrase taken from that section of the data [39].

Table 4. Results from the Privacy Concern Rating Task

ID	PVC Types	Conditions				
		Public	*Human VATs Knowingly*	*Human VATs Unknowingly*	*AI VATs Knowingly*	*AI VATs Unknowingly*
	Financial					
1	Account Information	**4.6**	2.8	3.4	2.5	3.1
	Medical					
2	Medical Information (Any)	**4.2**	2.9	3.4	2.8	3.2
3	Pill Bottle w. Name, Address, Other.	**4.1**	2.1	2.5	2.1	2.5
4	Pregnancy Test Result	**3.8**	2.6	3.2	2.3	2.8
	People					
5	Naked Body	**4.1**	**4.0**	**4.1**	3.3	3.5
6	Face	2.6	1.7	2.1	1.8	1.9
7	Framed Photo	2.4	1.9	2.1	1.8	2.1
8	Tattoo	1.8	1.4	1.7	1.5	1.6
	Location					
9*	Letter w. Address, Name	**3.7**	2.1	2.7	2.1	2.7
10*	Misc. Papers w. Address, Name	3.0	1.9	2.1	1.9	2.1
11	Address	2.9	1.8	2.0	1.8	2.1
12	Physical Position	2.2	1.4	1.6	1.2	1.4
13	Receipt with an Address	1.9	1.1	1.4	1.2	1.4
14	Local Street Sign	1.7	1.2	1.2	1.0	1.1
15	Library Book w. Branch Name	1.6	1.1	1.2	1.1	1.3
16	Newspaper with City Name	1.5	1.1	1.1	1.0	1.1
	Identification					
9*	Letter w. Address, Name	**3.7**	2.1	2.7	2.1	2.7
10*	Misc. Papers w. Address, Name	3.0	1.9	2.1	1.9	2.1
17	Name	2.7	1.8	2.1	1.7	2.0
18	License Plate Number	2.4	1.5	1.6	1.5	1.7
19	Business Card w. Contact Info.	1.6	1.1	1.2	1.2	1.3
	Computer/Online Access					
20	Computer Screen w. Username	2.8	1.5	1.9	1.6	2.0
	Affiliation					
21	Clothing with a Logo	1.3	1.3	1.4	1.1	1.3
	Average Score	**2.8**	**1.8**	**2.1**	**1.8**	**1.8**

[Concern Rating Index: 1 = Not/Doesn't faze me; 2 = Mildly/Think about it after the fact; 3 = Concerned/Discuss it with other people; 4 = Very/Develop strategies to change my behavior; 5 = Extremely/Change my behavior immediately]. This table shows 21 PVC types clustered according to seven higher-level PVC Clusters and ordered by decreasing privacy concern in the context of public sharing. Overall, participants ranked public disclosure as the most concerning context, followed by unknowingly sharing with human-powered VATs. When shared publicly, Financial Account Information (ID 1) received the highest concern score (Ave. 4.6/5.0), though participants rated PVC type ID 5 (Naked Body) as of great concern across all conditions (3.8/5.0–averaged). [*] Indicates a repeated PVC type because it falls under two clusters.

Public: On average, participants rated their concern about Financial Account Information being made publicly available as 4.6 out of 5 (Table 4, ID 1). Sixteen participants rated the public availability of their Financial Account Information as extremely concerning, due to the possibility of *Financial Theft*, an *Undefined Threat/Consequence*, or *Identity Theft*. Participants related their concerns to a fear of their *Lack of Personal Management* over their information (caused by their own actions), a sense of *Loss of Control or Agency* (caused by others), or *Social Judgement*. In one instance, a participant indicated that Financial Account Information is an *Intimate Personal Experience*.

Human-powered VATs: Concern was dramatically lower when sharing financial PVC *knowingly* with human-powered VAT; i.e., a drop from 4.6 in the public context to an average of 2.8. Those who expressed concern or extreme concern specified *Financial Theft*, *Unwanted Identity Disclosure*, and *Unknown Data Handling* as reasons. We attribute the majority of the responses which indicated lower concern to participants' *Need for Information* or their understanding of the *Professionalism* of the VAT, that their data would be *Protected by Policy*. That said, participants' concerns were higher (3.5) when their Financial Account Information would be shared *unknowingly* with a human-powered VAT. The primary reasons for this increase can be attributed to the participants' fear of *Lack of Personal Management* in that the sharing of this information was *Outside* [the realm of their] *Personal Awareness or Control*, and can result in *Loss of Control or Agency*.

AI-powered VATs: On average, participants' concerns when *knowingly* sharing PVC with AI-powered VATs was slightly lower than doing so with human-powered VATs. Only two participants expressed extreme concern with AI-powered VATs, based on fear of *Financial Theft* or *Unwanted Identity Disclosure*. Other concerns included *Unknown Data Handling* and *Multi-party Privacy Conflict*. Those who expressed less concern reasoned that they had a *Need for Information* or that it was *Common Practice* to use AI-powered services for this purpose. Moreover, others understood there would be *No Human Eyes on Data* or *Data on Device Only*. Still others expressed less concern due to the *Professionalism* of the service and the understanding they were *Protected by the Policies*. In the case that data would be shared *unknowingly* with human-powered and AI-powered VAT, the participants scores were higher then when shared *knowingly*. This increase in concern can be attributed to participants' fear of *Lack of Personal Management* and *Unknown Data Handling* in addition to many of the aforementioned concerns.

Medical Information: On average, participants were almost as concerned about Medical Information as Financial Account Information **(IDs 2-4)**, though for different reasons. For example, the participants who expressed extreme concern that their Medical Information **(ID 2)** would be publicly shared offered the following reasons: it reveals a *Intimate Personal Experience*, *Undefined Threat/Consequence*, *Social Judgement*, *Against HIPAA*[9], and *Multi-party Privacy Conflict*. Participants' concerns were lower when thinking about sharing Medical Information with human-powered or AI-powered VATs than publicly: 4.2 for sharing publicly versus 2.9 and 3.4 for sharing with human-powered VATs *knowingly* and *unknowingly* respectively **(ID 2)**. Participants' considerations for sharing with human-powered VATs included: *Professionalism* of the service, being *Protected by Policy*, a *Trust of Human Decency*, or simply because they have a *Needed for Information*. Considerations for sharing with AI-powered VATs *knowingly* included: *Data on Device Only*, *No Human Eyes on Data*, or *Anonymized Personal Data*. Similar to Financial Account Information, the prospect of *unknowingly* sharing medical PVC with either human-powered VATs or AI-powered VATs was slightly higher concern than when *knowingly* sharing the same information.

[9]The **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**, which is United States legislation that sets data privacy and security provisions for safeguarding medical information, such as medical records and other identifiable health information.

People: When considering images showing a person's body or face, including a Naked Body, a Face, a Framed Photo of people, or a picture of a Tattoo **(IDs 5-8)**, images showing a *Naked Body* were of greatest concern—with only slight variation in concerns across the condition that it would be shared publicly (4.1) or with human-powered VATs, *knowingly* (4.0) or *unknowingly* (4.1). The concerns participants expressed regarding the disclosure of an image of a Naked body included: *Damage to Reputation*, *Social Judgement*, *Disclosure of Identity*, or would be *Grounds for Termination of Use* of the VAT. In addition, they expressed the fear of *Lack of Personal Management*, *Multi-Party Privacy Conflicts*, along with the fact they would be *Unfamiliar with Person* providing the description and that they *Wouldn't Share Intentionally*. The score for sharing this PVC with an AI-powered VAT *knowingly* was lower because participants felt there were *No Human Eyes on Data* or because *Computers Can't Blush*, meaning a participant's actions would not cause embarrassment for the agents providing the description. In cases where participants might *unknowingly* share an image of a Naked Body, the average score was higher. This can be attributed to fear of *Lack of Personal Management* in addition to the other reasons noted for this cluster.

Location: This cluster included eight PVC types **(IDs 9-16)**. Publicly sharing paperwork with a Name and/or an Address were of highest concern for participants **(IDs 9-10)**. Participants also understood that sharing an address would be more concerning than one's Physical Position because an address could be used to locate their homes indefinitely, whereas their physical position may be temporary. As with other PVC clusters, participants were more concerned across all location PVCs about sharing *unknowingly* with AI-powered VATs rather than *knowingly*. We also observed that participants' concern about location-based information was higher when the content was more. For instance, participants showed low concern for newspapers with the name of their city **(ID 16)** or a local library branch **(ID 15)** (which were identified as *Public Information*), whereas Letters, Personal Names, or one's Address **(ID 9-10)** were of higher concern.

Identification. In this cluster, the most concerning PVC included a Letter with an Address and/or Name as well as Miscellaneous Papers with an Address and/or Name when shared publicly. While overall the License Plate **(ID 18)** rating fell between mildly concerning and concerning, some participants rated this License Plate as very or extremely concerning because they understood this information to be a risk if *Paired With Other Information/Metadata* and that it represented an *Unwanted Identity Disclosure* or an *Undefined Threat or Consequence*. We also commonly heard that by sharing License Plate information participants could be violating others' privacy and that they needed to protect others so that *Multi-party Privacy Conflicts* do not occur.

Computer/Online Access. On average, participants' were between mildly concerned and concerned (2.8 out of 5.0) about disclosure of their Username **(ID 20)**, particularly in the case that it was shared publicly or *unknowingly* with VATs. Participants were concerned sharing their username could result in *Unwanted Identity Disclosure*, or *Unwanted Human Viewing*. They also expressed fear of *Lack of Personal Management*, and that unintentional sharing would be *Outside Personal Awareness or Control*. We also heard concern about the threat that malicious actors could pose if Username information was *Paired With Other Information/Metadata*, e.g., passwords or location data.

Affiliation. One PVC type fits here: a piece of Clothing with a Logo **(ID 21)**. In the few instances participants gave a high rating to this PVC, the concerns centered on *Damage to Reputation*, or *Social Judgement*. Under the condition of sharing this PVC type *unknowingly* with human-powered or AI-powered VATs, participants worried the sharing would be *Outside Personal Awareness or Control* or cause fear related to *Lack of Personal Management*.

Table 5. The Ten Most Common Risk Factor Codes Applied to the Privacy Concern Rating Task Short-answer Responses

ID	Code	Definitions of the Risk Factors Impacting the Participant's Privacy Concerns	Count	%
1	Unknown Data Handling	A participant's assessment that they are unaware of what happens to shared images and videos and/or what is specified in the company's privacy policies.	115	12.8%
2	Undefined Threat or Consequence	A participant's assessment that there is a PVC disclosure risk, but no statement about how the person was impacted by that risk.	97	10.8%
3	Multi-party Privacy Conflict	A participant's assessment that sharing another person's PVC can cause harm and/or the need to augment their behavior to mitigate or eliminate risk for another.	94	10.4%
4	Reveals Intimate Personal Experience	A participant's assessment that disclosure of information will expose something that they only share with their closest family/community members (as opposed to acquaintances or strangers).	89	9.9%
5	Unwanted Identity Disclosure	A participant's assessment that there is a possibility that visual data/ digital records containing recognizable features of one's body, e.g., Face, can be accessed and used in a way that goes against their desires, morals, or values, and is done so without their knowing or consent, e.g., authority/ability to choose.	87	9.7%
6	Outside Personal Awareness/Control	A participant's assessment that the disclosure of information would occur without their conscious choice or decision.	80	8.9%
7	Lack of Personal Management	A participant's assessment or even self-judgment that the disclosure would mean the person did not organize the environment to the standard needed to protect one's privacy while using a VAT.	62	6.9%
8	Unwanted Identification of Location	A participant's assessment that another person would use shared information to find where that person resides.	56	6.2%
9	Loss of Control or Agency	A participant's assessment that disclosure of information would reduce their ability to manage their personal affairs.	40	4.4%
10	Social Judgement	A participant's assessment that disclosure of information (or a certain behavior related to sharing an image with PVC) would entice a negative critique from others, causing personal embarrassment or other psychological impact.	40	4.4%
	All other codes	Damage to Reputation; Theft of Financial Resources Inaccuracy of Technology; Lack of Personal Management; Not Socially Acceptable; Theft of Identity; Unwanted Human Viewing; Consent Not Granted; Against HIPAA; Betrayal of Trust; Betrayal Personal Rights; Unwanted Use of Data to Train; Grounds for Termination of Use; System Vulnerable to Hacks (Definitions can be found in the supplementary materials).	141	15.6%

Seven hundred and sixty (or 87%) of the 901 short-answer responses coded as Privacy Concern Rating Task fell under these 10 codes.

4.2.2 The Most Commonly Considered Risk in Sharing PVC: Unknown Data Handling. The participants in our study provided 1,890 short-answer responses during the privacy concern rating task. We coded 901 of these as adding a sense of *risk* to their visual privacy. The most common of these risks are defined in Table 5, with the top one being *Unknown Data Handling* with 115 or 12.8% of the 901 risk-related responses. In a second round of thematic analysis [22] of the 115

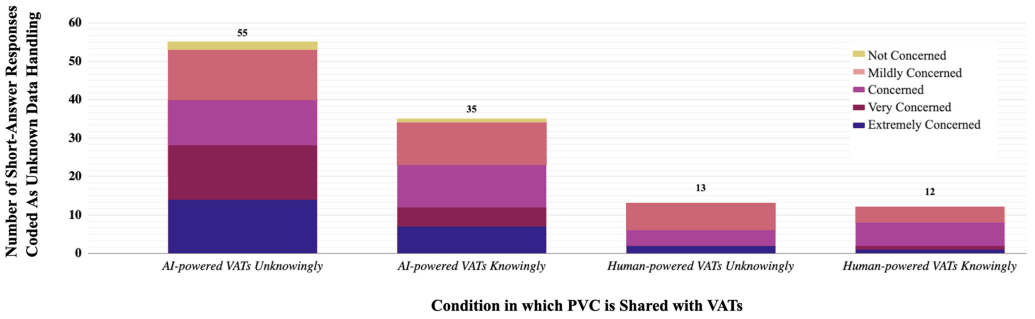

Fig. 1. The 115 short-answer responses coded as *Unknown Data Handling* distributed according to the condition in which PVC is shared and the associated privacy concern rating. The risk of Unknown Data Handling was mentioned far more often with AI-powered VATs than with human-powered VATs. For example, there were 55 instances of participants mentioning this risk when sharing *unknowingly* with AI-powered VATs vs. only 13 instances when sharing *unknowingly* with human-powered VATs.

risk responses, we performed a secondary thematic analysis [22]. From this analysis, we found that participants are unaware of (1) what happens to their images and videos once they have been shared, and/or (2) what security precautions VATs take to safeguard their PVC. For example, when talking about *unknowingly* sharing an image containing a Face with AI-powered VATs **(ID 6)**, P06 reflected *"I don't think they save my information...maybe I have the wrong idea of AI; but I don't know."* Under the same condition, but with a License Plate **(ID 18)**, P15 asked, *"Well, with technology things get out there. How are my images used?"*. In the context of a Pregnancy Test **(ID 4)**, P04 reflected, *"I don't know where are they storing it [images] or transmitting it* [a computer screen showing a username **(ID 20)**]*...If I knew exactly what the limits are on how the information is used and shared, I would drop it [my score] down low, but I don't know what their rules are, really"*. Similarly, but for Financial Account Information **(ID 1)**, P10 said *"I don't think they are being shared, but I don't know"*.

Those who mentioned not having a clear understanding of VATs' security precautions, shared statements such as *"With an AI app, I have thought about it. I don't know if it's saved on a computer. I wouldn't totally think that there's NO way it [PVC] could ever be shared or found out by anybody"* (P16 reflecting on financial account information, **ID 1**. Reflecting on how AI is developed, P17 also raised a question about the security of his images containing Misc. Papers w. Address, Name **(ID 10)**: *"AI is still made by people, they are using the internet for weapons and I don't know how it is protected"*. Finally, statements demonstrated participants' awareness of VAT companies' privacy policies, though not necessarily that they had read those policies. For example, regarding Medical Information **(ID 2)**, P10 said, *"I just realized I don't know their privacy policy because I don't read it. They could access my health information. I should probably read the statements!"*. It is not surprising that P10 (or the other participants in our study reported not read privacy policies; prior works tells us that privacy policies are notoriously difficult to read and inaccessible to most media consumers, e.g., [62].

These findings and the findings shown in Figure 1—the distribution of responses coded as *Unknown Data Handling* across VAT types and sharing conditions, indicate that VAT users are more concerned and have more questions about how their data is handled for AI-powered VATs than human-powered VATs, particularly under the condition that data is shared with AI *unknowingly*. A possible reason for blind people's concerns for sharing data with AI-powered VATs is that they expect for a person to see their data when it is shared with a human-powered VAT but not for AI-powered VATs, i.e., *No Eyes on Data*, which could be contested as data scientists

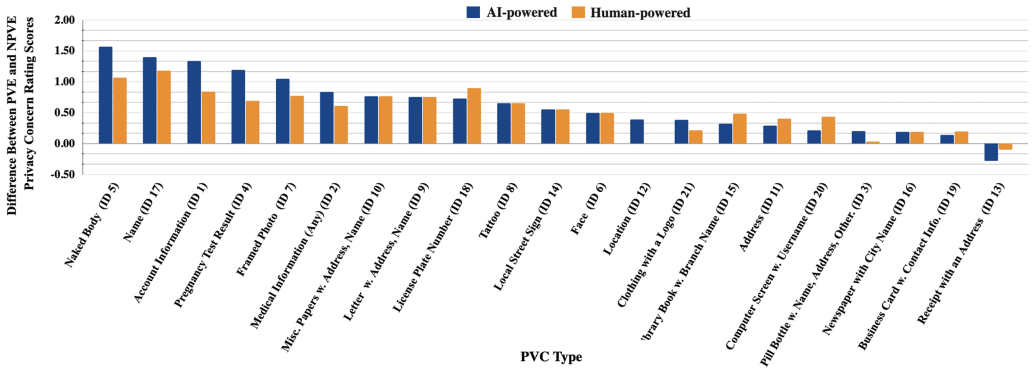

Fig. 2. Difference in the *Privacy Concern Rating Scores* between participants with *prior visual experience* and those with *no prior visual experience* according to VAT type. Positive differences indicate that participants with *prior visual experience* were more concerned about privacy than those without, which was the case for all but one PVC type. The greatest difference between the two participant groups was when sharing images that show a Naked Body **(ID 5)** with AI-powered VATs. For this PVC type, the privacy concern ratings of participants with *prior visual experience* are approximately 1.5 points higher than those with *no prior visual experience*. Across all PVC types the average difference in privacy concern ratings between participants with prior visual experience and no prior visual experience is .62 (SD = .48) for AI-powered VATs, and .53 (SD = .35) for human-powered VATs.

commonly explore data to develop AI-powered services. All the while, to our understanding, VAT companies do not publicly disclose who within VAT organizations and their affiliated third parties have direct access to PVC. A second reason for blind people's concerns for sharing data with AI-powered VATs could be related to their knowledge and understanding of VATs data security infrastructure and protocols.

4.2.3 Impact of Prior Visual Experience on Privacy Concern Ratings. Throughout the analyses of the semi-structured interview data and the short-answer responses, we began to see evidence that a person's prior visual experience influences their privacy concerns. As such, we analyzed participants' privacy concern rating scores according to whether participants had acquired blindness at age 15 or after (n = 9) and thus had *prior visual experience* or were blind from birth (n = 9) and thus had *no prior visual experience*.

Figure 2 shows this analysis broken down by human-powered vs. AI-powered VATs, but collapsed across the conditions of *knowingly* and *unknowingly* sharing data as these scores followed similar trends to the aggregate scores. For both human-powered and AI-powered VATs, and across all but one PVC type, participants with *prior visual experience* were more concerned about privacy than those with *no prior visual experience*. The only exception is for Receipt with an Address (**ID 13**), where the raw average concern ratings were higher for people with *no prior visual experience* than those with *prior visual experience*: 0.3 higher on average for sharing this PVC type with AI-powered VATs and 0.03 higher for human-powered VATs. These findings indicate that prior visual experience is an important factor affecting visual privacy concerns, perhaps because visual experiences provide a stronger sense of information that *can be* gleaned visually from an object and provide a broader range of reference points—a question we leave to be explored in future research.

4.3 Summary

This section primarily addresses RQ2, *Which PVC types are of most concern to people who are blind, generally, as well as when using human-powered versus AI-powered VATs?*, and RQ3, *How does the*

intentionality of privacy disclosures affect what they consider to be PVC when using VATs? The PVC type of greatest concern was *Naked Body* **(ID 5)** across all conditions, but particularly salient when this PVC is shared with human-powered VATs *unknowingly* with a privacy concern scale of 4.1. Towards further answering RQ2, we identified that participants rated their concern consistently high when sharing *Financial Account Information*, *Medical Information*, *Pill Bottles with Names and Addresses*, and *Pregnancy Tests*—across all sharing contexts. Addressing RQ3, we found that for both human-powered and AI-powered VATs, participants generally rated *unknowingly* sharing PVC as more concerning than *knowingly* sharing it.

Deepening our understanding of the PVC types that are of most concern, in Section 4.2.3 we also presented evidence that people with *prior visual experience* were generally more concerned about their visual privacy than people with *no prior visual experience*—indicating that this is another factor that VAT companies should be aware of when handling users' visual data.

Findings in this section also expanded on the factors we identified in Section 3 as impacting blind people's privacy concerns, particularly in terms of perceived risks (RQ1) (e.g., *Unknown Data Handling*). These findings can be used by VATs to better understand their users and develop safeguards that address the factors causing the greatest privacy concerns. For instance, our secondary analysis of the most common of these risks—*Unknown Data Handling*, showed that much of the concern arose with AI-powered VATs though we applied this code across all contextual conditions (and most PVC types). This indicates that efforts should be taken to better inform users about what happens to their personal visual data.

5 PRIVACY POLICY ANALYSIS

The previous sections (Study 1) identified that blind people's visual privacy concerns when using VATs are commonly related to their familiarity (lack thereof) VAT companies' data handling practices, e.g., *Unknown Data Handling*. To understand how well VAT companies are addressing these concerns, specifically the risk around data collection and processing, we performed a content analysis of 13 VAT companies' privacy policies to answer RQ4: *What are VAT companies communicating to users about the collection and processing of visual data, as embodied in their privacy policies?* (RQ4). Privacy policies are legal documents that disclose how customers' data is handled, such as the recording, retention, use, and dissemination of their data [94], and these documents are the primary source for VAT users to learn how the companies handle their personal visual data. From this analysis we suggest strategies to better inform VAT users of the implications associated with sharing PVC for access to information.

5.1 Methods

In what follows, we describe how we identified the companies to include in our study, our process for curating their privacy policies, our annotation protocol, and our approach to analyzing the policies.

5.1.1 Data Collection. Our dataset includes privacy policies from 13 companies as listed in Table 6. This set of companies covers popular camera-based applications used by blind people, as represented in the academic literature on visual assistance (e.g., [40, 64, 95]) and based on our experience conducting research with blind people: *Aira, Be My Eyes, BeSpecular, KNFB Reader, Lookout, LookTel MoneyReader/Recognizer, OrCam MyEye, Seeing AI*, and *TapTapSee*. These applications support a variety of use cases, types of camera-based devices, and visual data input types (images and videos) as shown in Table 6.

Table 6. The 13 Companies Whose Privacy Policies We Analyzed, Along with VAT Product Names, Form Factors (Mobile, Wearable, Desktop), the Type of Visual Data They Accept (Images, Video), and the Type of Intelligence Used to Provide Visual Assistance (Human, Artificial)

Name	Application	Camera Form Factor	Visual Data Type		Intelligence Type		Use Statistics
			Image	*Video*	*Human*	*Artificial*	
Aira	Aira	Mobile Device, Glasses		X	X	X	"Thousands of users" [64]
Be My Eyes	Be My Eyes	Mobile Device	X		X		"More than 100,000 users" [34]
BeSpecular	BeSpecular	Mobile Device	X		X		"Thousands [15]
LookTel	LookTel Money Reader	Mobile Device	X	X		X	Not Available
	LookTel Recognizer	Mobile Device	X				Not Available
OrCam	OrCam MyEye	Glasses		X		X	Not Available
	OrCamRead	Handheld "Smart Camera"	X			X	Not Available
Sensotec	KNFB Reader	Mobile Device	X			X	Not Available
TapTapSee	TapTapSee	Mobile Device	X	X		X	Not Available
Google	Lookout	Mobile Device	X			X	Not Available
Microsoft	Seeing AI	Mobile Device	X			X	"Used 20 million times" [31]
Adobe	Adobe Accessibilty	Unspecified	X	X		X	Not Available
Amazon	Amazon Rekognition	Unspecified	X	X		X	Not Available
Apple	VoiceOver Recognition	Unspecified	X			X	Not Available
Facebook	Automatic Alt Text	Unspecified	X	X		X	Not Available

We further expanded the set of privacy policies by identifying companies that have interests in both accessibility and computer vision[10] even if they do not currently have a popular VAT product. We made this choice based on the understanding that AI-powered (automated) visual assistance is a growing trend within industry and accessibility is a key motivator for development[11] To do so, we identified two top conferences in accessibility (the CSUN Assistive Technology Conference 2019 [113] and ACM SIGACCESS Conference on Computers and Accessibility (ASSETS) 2019 [10]), and the top conference in computer vision (IEEE Conference on Computer Vision and Pattern Recognition (CVPR) 2019 [36]). For each conference, we reviewed the sponsors as listed on the public website: 107 for CVPR, 12 for CSUN, and 9 for ASSETS. The following companies sponsored both CVPR and at least one of the accessibility conferences: *Apple, Adobe, Amazon, Google, Facebook*, and *Microsoft*. While Microsoft and Google were already in our company set because of related VATs (Seeing AI and Lookout, respectively), we added the remaining four companies for a total of 13: Apple, Adobe, Amazon, and Facebook.

For each of these 13 companies, a research team member manually gathered the privacy policy from the company's website in Fall 2019. When visual assistance was one of many products offered by a company and did not have a unique privacy policy associated with it, we looked to the parent company's privacy policy; e.g., for Seeing AI we downloaded Microsoft's privacy policy. Each company's entire privacy policy was collected for later analysis.

5.1.2 Analysis. To systematically evaluate what VAT companies communicate to users about how their personal visual data is handled, we first developed an annotation protocol. Two sighted researchers on our team, with post-graduate education and varied experiences reading privacy policies,[12] independently read three companies' privacy policy statements (Aira, Facebook, and Google) to gain familiarity with the structure and language used within privacy policy documents, and determine whether a systematic review of the policies would yield interesting results. Through

[10]Computer Vision is a sub-field of AI about making computers that can analyze visual content.

[11]For instance, the Sight Tech Global conference was launched in 2020 with the motivation of "Shaping New Technologies to Create a More Accessible World for People with Blindness and Visual Impairments" [32].

[12]Prior to the onset of the study, one researcher on our team (with a PhD) reported never having read a privacy policy; the other, who is currently completing a PhD, reported having extensive experience locating and reading privacy policies, in the context of conducting research and training older adults to develop health literacy skills.

Table 7. Shown are the Prompts Used By Two Annotators to Systematically Analyze 13 VAT Companies' Privacy Policies

ID	Prompt	Definition
1	Is data collected?	If the company states whether they record data (e.g., "data", "cookies", "personally identifiable information", "location", "email", "phone numbers", "images", "videos").
2	Is video collected?	If the company states whether they collect/record videos.
3	Are images collected?	If the company states whether they collect images.
4	How long is data retained?	If company discloses the duration in which they will store the data they record for **(A)** the generic term data as well as **(B)** the sub-category of visual data.
5	Is data used to train algorithms?	If the company discloses whether the data is used to develop automated approaches to perform their services for **(A)** the generic term data as well as **(B)** the sub-category of visual data. Language used may explicitly state for algorithm "training" as well as other more ambiguous terms such as "improve the service" for the user.
6	Is data shared with third parties?	If the company discloses whether they disseminate the data they record with a person or group besides the two primarily involved in a situation (the user and the service provider) for **(A)** the generic term data as well as **(B)** the sub-category of visual data.
7	Can data be deleted?	If the company discloses whether users can opt to delete their data for **(A)** the generic term data as well as **(B)** the sub-category of visual data.
8	Can users opt out of data being collected?	If the company discloses whether users can opt out of their data being collected for **(A)** the generic term data as well as **(B)** the sub-category of visual data.

several iterations, our team collectively developed, refined, and finalized the coding scheme to annotate the policies in our dataset.

The final schema included a set of prompts Table 7, which focused on what companies communicated to users about the types of data collected, users' choices to opt out or delete their data, and the retention of visual data including its storage, use for AI development, and use by third parties. Some of these prompts had sub-prompts, which we refer to as sub-prompt 'A' and sub-prompt 'B'. Two researchers (annotators) independently read and located in each of the 13 companies' privacy policy statements any text that addressed each prompt. Each annotator assigned one of three scores to each prompt: a score of 1 to indicate that the privacy policy *"contains information that addresses the question"*, a score of 0 to indicate that the policy *"explicitly states that the recording of data or privacy protection does NOT occur"*, and -1 to indicate that the policy *"does not provide information that helps answer the question"*. As a result, for each policy, both annotators produced 13 scores to cover all the prompts and sub-prompts. In total, each annotator assigned 169 scores across the 13 policies (i.e., $13 \times 13 = 169$).

Four of the co-authors met to analyze the results, and found that neither annotator had assigned a score of 0 to any prompts across all privacy policies; that is, none of the companies explicitly stated that they did *not* engage in data handling practices. Consequently, we retrospectively shifted all scores to reflect a binary rating system: **1** to indicate the policy provided information that the data handling occurs, and $\mathbf{-1}$ to indicate when the annotator could not find any information to address the prompt in the policy.

We calculated Cohen's kappa to measure inter-rater reliability between the two independent annotators. Across all prompts, we achieved an average inter-rater reliability of 0.84, which signifies a

moderate to high degree of agreement (range: .61–1.0). To address the 26 out of 182 instances when the two researchers' annotations differed (i.e., 14% of all prompts), they collaboratively reviewed the privacy policies, and came to an agreement about the information communicated within.

5.1.3 Policy Validation. To ensure that the data was current at the time of submitting this journal article, in May 2021 the lead author revisited the source of each policy and collected a new copy as described above. To identify updates to the policies, we first observed if there was a change in the publication date, then compared the initial 2019 dataset to the 2021 policies on the VAT companies websites using the *Track Changes->Compare Documents* tool in Microsoft Word. Eight of the 13 companies had updated their policies between December 2019 and May 2021.[13] We observed only one change that corresponded to our annotation protocol: Amazon's privacy policy now directly specifies that video and image data are collected, e.g., *"When you use our voice, image and camera services, we use your voice input, images, videos, and other personal information to respond to your requests, provide the requested service to you, and improve our services."* We account for this change in the presentation of the findings in Table 8 and the corresponding text.

5.2 Results

To address RQ4, *What are VAT companies communicating to users about the collection and processing of visual data,as embodied in their privacy policies?*, we share results below with respect to (1) the *notice* that is/is not communicated about the collection, length of retention, use, and dissemination of visual data (i.e., images or videos), and (2) the *choices* that are/are not communicated to users about opting-out of having their personal *visual* data collected and to have their personal visual data deleted. Table 8 presents the findings according to each VAT company and each prompt, and the Cohen's kappa inter-rater reliability score from our analysis.

5.2.1 Notice.

Data Collected. All of the companies in our dataset provide notice that *general personal data* is collected. However, only nine of the 13 policies specified that the personal data collected includes *video* (Prompt 2) or *image* (Prompt 3) data. This includes four of the seven companies that have privacy policies specific to a visual assistance applications: Aira, Be My Eyes, BeSpecular, and TapTapSee. The companies with umbrella policies that report on personal visual data collection include Adobe, Amazon, Facebook, Google, and Microsoft, though it is unclear which of their product lines or services collect users' visual data. If a company indicates in its policy that images are collected, the company also is likely to collect video (with the exception of BeSpecular, who reports on the collection of image data but not video data). Finally, those who do *not* indicate that they collect images include LookTel, OrCam, Sensotech, and Apple.

Length of Data Retention: Eight of the 13 companies communicate information about the data retention period for *general personal data*, including companies with umbrella policies (Adobe, Facebook) and policies specific to a visual assistance technology (Aira, BeSpecular, OrCam, Sensotech, TapTapSee, and Google). However, neither annotator found a single instance mentioning the retention period for visual data specifically.

[13]The VAT companies whose privacy policies were updated include: (1) Be My Eyes (latest update May 2020), (2) OrCam MyEye (latest update June 2020), (3) Google (latest update February 2021), (4) Amazon (latest update February 2021), (5) Adobe (latest update December 2020), (6) Apple (latest update December 2020), (7) Facebook (latest update January 2021), and 8) Microsoft (latest update April 2021). The VAT companies whose privacy policies had not been updated include: (1) Aira (latest update June 2018), (2) Be Specular (latest update May 2016), (3) KNFB Reader (latest update September 2016), (4) LookTel Money Reader (no date), and (5) TapTapSee (latest update August 2013).

Table 8. Results of the Privacy Policy Analysis, Showing Whether Companies Provide ***notice*** About Collecting Users' Data (Prompts 1-3), the Length of Data Retention (Prompt 4), the Use of Data to Train AI (Prompt 5), and the Dissemination of Data to Third Parties (Prompt 6), as well as the ***choice*** these Companies Provide Users for Deleting Their Data (Prompt 7) and opting-out of having their Data Collected (Prompt 8)

	Collect			**Retain**		**Train AI**		**Third Party**		**Delete**		**Opt-Out**	
	1	*2*	*3*	*4a*	*4b*	*5a*	*5b*	*6a*	*6b*	*7a*	*7b*	*8a*	*8b*
	Any	*Video*	*Image*	*Any*	*Visual*	*Any*	*Visual*	*Any*	*Visual*	*Any*	*Visual*	*Any*	*Visual*
Company													
Aira	Yes	Yes	Yes	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No
Be My Eyes	Yes	Yes	Yes	No	No	Yes	No	Yes	Yes	Yes	No	No	No
BeSpecular	Yes	No	Yes	Yes	No	No	No	Yes	No	Yes	No	No	No
LookTel	Yes	No	No	No	No	No	No	No	No	Yes	No	Yes	No
OrCam	Yes	No	No	Yes	No	Yes	No	Yes	No	Yes	No	No	No
Sensotech	Yes	No	No	Yes	No	No	No	No	No	Yes	No	No	No
TapTapSee	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	No	No
Google	Yes	Yes	Yes	Yes	No	Yes	No	No	No	Yes	No	No	No
Microsoft	Yes	Yes	Yes	No	No	Yes	No	Yes	No	No	No	Yes	No
Adobe	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No	Yes	Yes	Yes	No
Amazon	Yes	**Yes**	**Yes**	No	No	No	No	Yes	No	No	No	Yes	No
Apple	Yes	No	No	No	No	Yes	No	Yes	No	Yes	No	Yes	No
Facebook	Yes	Yes	Yes	Yes	No	Yes	No	Yes	No	Yes	No	No	No
Totals													
Yes	13/13	8/13	9/13	8/13	0/13	9/13	2/13	10/13	2/13	10/13	1/13	6/13	0/13
No	0/13	5/13	4/13	5/13	13/13	4/13	11/13	3/13	11/13	3/13	12/13	7/13	13/13
Inter-rater Reliability Measures													
Cohen's kappa	1.0	.92	.84	.84	.77	1.00	.77	.92	.77	.61	.77	.84	.84

For prompts 4-8, each question comes with two sub-prompts, the first one related to data in general and the second one specifically looking at handling of visual data. **Yes** = instances when the policy included the information; **No** = instances when the policy did not include the information.

Use of Data to Train Services: Prompt 5 centers on whether companies give notice about the use of the data they collect to train AI algorithms. Eight of the 13 companies indicate that they use *general personal data* to train AI (Aira, BeSpecular, OrCam, Sensotech, TapTapSee, Google, Microsoft), yet only two of these companies specify they use *personal visual data*. One of the two companies, TapTapSee, has a policy specific to their visual assistance application. The other company (Adobe) has an umbrella privacy policy that does not specify if the data collected is used in this way. The five companies in our dataset that did not provide information about the use of data (general or visual) to train AI include: Be My Eyes, LookTel, Microsoft, Amazon, and Apple.

Sharing of Data with Third Parties. Prompt 6 deals with whether companies disseminate *personal visual data* to third parties, such as other companies, organizations, independent contractors, or individuals outside of the primary organization. The analysis revealed that two company's privacy policies clearly indicate that *personal visual data* are shared with third parties (Be My Eyes and TapTapSee). The two annotators could not find information about whether *personal visual data* are shared from the other 11 companies' privacy policies.

5.2.2 Choice.

Deletion of Data. Prompt 7 pertains to whether companies' privacy policies include information about the choices users have for deleting their *personal visual data*. Twelve of the 13 companies do not provide such information—Adobe is the only one that does. Ten of the 13 companies communicate that users can delete *general personal data*.

Opting-out of Data Collection. The final prompt centers on whether the privacy policies include information about users' choice to opt out of having their data collected. None of the companies provide this information for *personal visual data*, and only six of the policies communicate that users can opt out of *general personal data* collection.

5.2.3 Summary. This study involved an analysis of 13 VAT companies' privacy policies, motivated by the aim of understanding what companies communicate to users about the collection and processing of their personal visual data. The findings reveal that VAT companies rarely provide clear "Notice and Choice" to users about what happens to their images and videos. Next, we discuss the implications of these findings paired with the those from Sections 3 and 4.

6 DISCUSSION

In this section, we summarize findings from Study 1 and Study 2, and then address how the findings fit within the context of the existing data regulation and contemporary trends in privacy-preserving technology design. Finally, we provide recommendations for how our human-centered research may be used to inform the development of human-powered and AI-powered VATs that offer privacy safeguards, i.e., are privacy-protective "by design".

6.1 Blind VAT Users' Privacy Concerns for AI-powered vs. Human-powered VATs

The semi-structured interviews (Section 3) affirmed prior work's [8, 9] finding that blind people have privacy concerns when using both human-powered and AI-powered VATs. The factors impacting these privacy concerns (RQ1) fall under three overarching categories: (1) users' understanding of how VATs provide the services, (2) users' perceptions of the impact of sharing PVC to their personal well-being or social relationships, and (3) users' assessments of how VAT services adhere to their values or raise values-based questions. Under each of these categories we identified factors they deemed to *benefit* their sense of privacy (as summarized in Table 2) and factors that introduce *risk* into participants' sense of privacy.

Benefits to VAT Users' Visual Privacy: These findings show that blind people value, and directly benefit from the *Anonymity* that both human-powered and AI-powered VATs provide. AI-powered VATs are perceived as providing greater anonymity than human-powered VATs as the data is not seen by close social ties—a finding that affirms findings by Akter et al. [9]. They viewed AI-powered VATs as an agent that mediates *Social Judgement*, whereas they viewed human-powered VATs as increasing the risk of social judgment–despite the anonymity provided. Participants also valued the *Interactivity* that human-powered VATs provide and perceived that the *Professionalism* of the sighted assistants bolsters their privacy.

Visual Privacy Risks for VAT Users: Findings from our open-ended interview questions, as well as the Privacy Concern Rating Task short answer-responses (Section 4.1.2) show that blind people perceive that their lack of understanding of if, how, and why VAT companies collect and process their data introduce a risk to their sense of visual privacy (e.g., *Unknown Data Handling*). This risk factor is pertinent for both human and AI-powered VATs (Section 2), and is the top (of 24) risk factors impacting VAT users privacy concerns when sharing PVC in their visual media *knowingly* or *unknowingly* for information access (Table 5) for both VAT types (Section 1). Our findings also show that VAT users are concerned about sharing 19 types of PVC, in part due to the *Unknown Data Handling* factor. The concern about *Unknown Data Handling* is most prevalent in the scenario that PVC is shared with AI-powered VATs. This may be due to an understanding that developing AI-powered visual assistance depends on large amounts of data whereas human visual assistance may not require the same data configurations and training to generate useful descriptions. Additionally, while contemporary media commonly reference the need for collecting

and processing user data to improve automated technologies, it is less clear how sighted assistants are trained [64]. Following Lee et al. [64], future work may be conducted to reveal what information is used to train visual sighted assistants, albeit with greater emphasis on how they are trained to accurately provide visual assistance *while* preserving users' privacy, versus the methods and data required to train AI-powered VATs.

In summary, both human-powered and AI-powered VAT companies may benefit from following our recommendations below regarding privacy education for users, greater transparency in their data collection and processing, and support public-facing research to reveal the data and skills are needed to train privacy-preserving VATs to support autonomy and the reduction of social judgment (as described in more detail in Section 6.4).

6.2 Additional Contextual Factors that Influence VAT Users' Visual Privacy

As detailed above, we explored three types of contextual factors that influence blind VAT users' sense of visual privacy when using VATs, e.g., VAT type, PVC type, and sharing condition. Our extended analysis of the Privacy Concern Rating Task data (Sections 4.2.3) offer preliminary insight that a persons' prior visual experience is another factor that influences their visual privacy perceptions when using VATs. We found that people who have acquired blindness (prior visual experience) have more privacy concerns then people who were born blind (no prior visual experience) across all but one PVC type. These findings have implications for how VAT companies can tailor their privacy-preserving services to meet a variety of VAT users' privacy concerns, develop methods for users to personalize the privacy-preserving features embedded into VATs, and even develop specialized educational resources for informing users of the measures taken to safeguard users' personal visual data. Our findings indicate that privacy needs to be understood and investigated as something that is highly contextual, varies based on social norms, and is variable based on the combination of factors influencing the person at the time [76].

6.3 VAT Companies' Communication to Users About Data Collection and Processing

We conducted an analysis of 13 VAT companies' privacy policies to further understand what VAT companies communicate to users about the collection and processing of their personal visual data (Study 2) in light of how frequently we heard VAT users explain their lack of understanding of how VAT companies collect and process their personal visual data in Study 1, Sections 3 and 4. Our analysis in Study 2 showed that seven of the 13 companies in our dataset do not communicate whether they collect images and video, and none of the companies provide notice about the retention of *personal visual data*. Only one policy in our dataset specifically indicated that users can delete their images and/or videos, but none provide the choice to opt out of it being collected. Only two companies mention whether they use images and/or video to train AI, and only two companies mention that they sell images and/or videos to third parties—both of which do.

Based on these findings, a concern is that VAT companies that collect and share users' personal visual data, neglect to remove PVC from images and videos before they are stored and shared. For instance, in a privacy policy of a human-powered VAT in our dataset we read, *"When we provide video streams to third parties we will anonymize them* ***as much as possible****. That means we will strip the file of any data that could be used to personally identify you.* ***We cannot, however, strip or edit the content of the video stream****. So if you film yourself, film your location (for example, if the Eiffel Tower is behind you), or verbally give your name or your location on the video stream, for example, that information may be shared."*

Accordingly, VAT users' personal visual data may be shared with VATs without users knowing who the recipients will be (e.g., 3rd parties), for what purposes the data will be used, and whether proper privacy safeguards in place, thus (1) limiting their opportunity to provide *informed consent*

(a concern that also emerged during the rating task), and (2) introducing a misalignment between what users' need and want to know to protect their privacy (e.g., the opportunity to provide consent to more information about what happens to their personal visual data when using VATs) and what the service provider offers. Below we provide details about how VATs can increase alignment with their users, including developing mechanisms to ensure that users have sufficient reference to provide *informed* consent.

6.4 Implications and Recommendations to Guide VAT Development

Our findings have unique implications for VAT users and companies because blind people share their visual data to gain access to information, and in doing so risk compromising their privacy. Here we provide recommendations for how VATs can be developed in ways that (1) increase VAT users' understanding of what happens to their personal visual data, thus also increasing VAT users' opportunity to provide informed consent, (2) take actions to further promote alignment between VAT users and VAT companies, and ultimately (3) account for the inherent contextual variables that influence users' privacy.

6.4.1 Designing VATs with Non-Visual Consent in Mind. Despite mounting criticism of the effectiveness of "Notice and Choice" for users (referred to in data regulation as "data subjects"), e.g., [84, 104], this paradigm is still the primary mechanism used to guide entities collecting users' data to inform users about the collection and processing of personal data [67]. Consent is an enactment of one's choice, and is one of the main legal basis for the treatment of personal data as outlined in the **General Data Protection Regulation (GDPR)**—a European Union-based law that demands that companies across all sectors of business adhere to practices that give individuals control over their personal data [67].[14] For consent to be valid in the context of personal data collection: (1) it must be freely given, e.g., "the individual must have a free choice and must be able to refuse or withdraw consent without being at a disadvantage", (2) users must be informed, e.g., users must receive information about the entity processing the data, the purposes for which the data is processed, the type of data that will be processed, the choice to withdraw consent, the use of the data for automated decision making, and the possible risks if data is transferred to third parties [80].

To the first point—consent must be given freely, results from our study indicate that VAT users may not be positioned to provide informed consent. Blind people use VATs, in the first place, to learn about the content contained within their images and videos, and it is unclear whether they are appropriately supported to know what information they disclose prior to consenting to the terms of service. Moreover, if users are uncertain or do not want to provide consent to the collection or

[14]Whereas GDPR offers omnibus data regulation, in United States data regulation is currently sectoral, meaning that data regulations are directed to specific industries, and depend on self-regulation more then governmental interference alone [67]. Despite the differences in approach to data regulation, the topic of privacy—in the context of the development of technical products and services and technology is at the core of data regulation and puts in place measures that require companies to communicate with users about the collection and sharing of personal data. In the 1880s Samuel D. Warren and Louis D. Brandeis issued a concern that instant photography and audio recorders, invented during that era, cause invasion into *"the sacred precincts of private and domestic life"* in the Harvard Review Article, "The Right to Privacy" [105]. Eighty-three years later, in a similar response to the emergence of new technologies and increasing data collection, the U.S. Department of Health, Education and Welfare submitted an article titled, "Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems". This report included a set of safeguards to address the lack of data and privacy protections under the law [27]. The **Organization for Economic Cooperation and Development (OECD)** later adopted these safeguards, to establish the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* and ultimately the ***Fair Information Practice Principles (FIPPs)*** [27]. The FIPPs, written in 1980, serve as a foundation for both the sectoral regulations in the United States and the omnibus data and privacy regulations in Europe.

processing of their personal visual data (generally) or for specific PVC types, their access to VATs or specific features may be withheld.

To the second point—users must be informed, results of our Study 1 indicate that VAT users do not consider themselves to be informed about VAT companies' handling of their data, even when they had read the privacy policies; readability of privacy policies is a well known issue, e.g., [62] that extends beyond the population we study here. Furthermore, our investigation in Study 2 showed that many VAT companies do not explicitly indicate that the personal data they collect comes in the form of images and videos, which reveal extensive amounts of personal data that people consider to be private, e.g., [53, 96]. The VAT companies that do provide notice about the collection of personal visual data indicate that they may not remove PVC from images and videos before they are stored and shared (as evidenced in Section 6.3).

Based on these considerations, we recommend that VAT companies proactively develop approaches to:

- Communicate to users the types of personal visual data VAT users (and others, e.g., [66]) consider to be private and under what conditions, whilst explaining the related risk factors.
- Explain to VAT users the validity of the perceived privacy risks based on the current robustness of their data security infrastructures.
- Communicate with VAT users about how they can successfully manage their environments and PVC before sharing visual media so unwanted disclosure is avoided.
- Provide users with contact information for customer support agents who can address privacy-related concerns.
- Provide VAT users with non-visually accessible tools that enable them to assess whether their images have PVC or not prior to obtaining visual assistance.
- Communicate to users, in real-time, when they have shared images and videos that contain personal data and provide in situ opportunities to provide consent before data is recorded or processed.
- Provide mechanisms to validate whether the consent users provide is *informed*, prior to the collection of data—from either the users' device or during a live session with a sighted visual assistant.

These measures may establish new social norms around *non-visual, visual privacy* that promote transparency and can be directly refined and conveyed by any VAT user. Future efforts may focus on user-centered research to observe VAT users' reactions to privacy and consent notifications, e.g., whether they would view such an intervention as adding helpful or hindering friction when trying to gain visual assistance, and when and how they would want this notice to be provided by human-powered and AI-powered VATs for different PVC content types. Additional efforts may focus on better understanding the ways in which VAT users want their PVC redacted or obfuscated–prior to gaining visual assistance, storage, or sharing (including use of data by third parties)—and how VATs can be personalized to match users' preferences.

6.4.2 Promoting Alignment Between VAT Users and VAT Companies through the 'Privacy by Design' Paradigm. As noted above, many VAT users commonly do not know what is specified in VAT companies privacy policies nor what is actually done with their personal visual data. Findings from Study 2 show that VAT companies rarely provide comprehensive notice or choice nor ensure that users comprehend their policies. This represents a misalignment between the information that users need for a sense of visual privacy and what information VATs provide. While the aforementioned recommendations (and other methods [59, 68, 98, 103, 112]), may be followed to improve alignment, we advocate that VAT companies shift away from simply following the 'notice

and choice paradigm' to following the more contemporary *'Privacy by Design'* paradigm. Privacy by Design is a *"a proactive approach, to make occurrences of privacy harms impractical in the first place. It demands that privacy be 'built in' during the design process"*, Pg. 1 [107] .

Our human-centered research takes a Privacy by Design approach by identifying what VAT users consider to benefit their sense of privacy and what they consider to add risks to their privacy (Section 3). Based on these findings, the following recommendations to may be used to design novel VATs that mitigate these privacy risks from the outset:

- Design VATs that eliminate users' experience of [*Social Judgement, Loss of Control or Agency, Lack of Personal Management*] when sharing private visual content with VATs.
- Design VATs so that users' sense of [*Autonomy*] is increased.
- Design VATs so that they inform users about the risks and benefits related to the collection and processing of personal visual data.
- Design VATs so they that account for users' changing privacy expectations.

These criteria may also be applied to refining the design of current VATs, and helping VAT users choose which VAT best matches their priorities—whether based on their goals for social and community well-being, their understanding of the service offering, or their underlying values.

6.4.3 Accounting for the Contextual Nature of Privacy in VAT Development. Another promising approach to developing VATs through the Privacy by Design paradigm is to account for the contextual nature of privacy during the delivery of visual assistance—visual privacy perceptions are greatly influenced by the contexts in which they share their personal data [53, 72, 76]—that result in personalized privacy-preserving services.

Study 1 demonstrates our effort to account for the contextual nature of privacy, during which we investigated (1) the type of VATs (human-powered or AI-powered, and (2) the intention of sharing (unknowingly or unknowingly). We provide new evidence related to the influence these factors on participants' privacy concerns when sharing 21 types of PVC with VATs, e.g., Table 4, as well as the influence of a person's prior visual experience on their sense of visual privacy—a factor that emerged during our investigation (Figure 2).

Our approach may be used by VAT companies to develop techniques that preserve users' visual privacy in a responsive and contextually aware manner, i.e., the ability to determine if an image with a specific PVC type should be collected and how it should be processed, as informed by the type of agent providing the visual assistance (human vs. AI), the intention of the disclosure, and/or the VAT user's prior visual experience. In the short-term, VAT companies may establish guidelines to inform VAT employees and volunteers how to respond to the presence of PVC to mitigate liability for the end user and the employees. In the long-term, we envision the development of privacy-preserving VATs that offer users the ability to specify which contextual understanding will benefit their sense of privacy the most and personally train VAT systems to handle their PVC accordingly.

6.5 Limitations and Future Research Directions

We now discuss limitations in our methods which point to valuable future research opportunities.

6.5.1 Study Design.

Study 1. During the Privacy Concern Rating Task, participants wanted more context for some of the PVC types to provide a confident answer. For instance, under the *Information Designation* subcategory, we identified 111 instances where participants stated their answer would change based on the specifics of the content, e.g., for images that show a tattoo where it would depend on what

the tattoo was of and where on the body it was located. In addition, there were 35 instances where participants indicated their scores would change based on the condition that a PVC was *Paired with Other Information*, such as in the case that a username was shared alongside the password, or that a picture of a face was paired with location metadata. When such considerations arose, we asked participants to provide a score that reflected their highest level of concern to account for the most sensitive outlier. We recommend validation of the findings we present in Section 4 with a larger sample size prior to being used in practice.

Study 2. There also were limitations to our analysis of the privacy policies for VAT companies. First, we used the "Notice and Choice" paradigm as a conceptual framework for our analysis as many of the companies in our sample are US-based, though should also adhere to GDPR. Second, during our analysis we observed that VAT companies do not communicate in their privacy policies about the collection and processing practices they do **NOT** engage in, leaving us with a binary approach to annotation. Future research may focus on conducting an in-depth content analysis of VAT companies' privacy policies to identify the rhetorical choices visual assistance technology companies make when authoring their privacy policies.[15] Future work may also consider an analysis according to the principle of "Privacy by Design" that guide GDPR, e.g., Article 25 data protection by design and by default [80]. Future work may extend our investigation of VAT companies' privacy policies by exploring how VAT users want VAT companies to author privacy policies—or to design alternative communication methods to provide assurance that their personal visual data is not being collected or processed (and if it is, how and why). Relatedly, it could be interesting to explore whether VAT users are concerned that some VAT companies have not updated their privacy policies since implementation of GDPR in 2018 (Section 5.1.3).

6.5.2 Investigating the Impact of the Identified and Additional Contextual Factors. Additional user studies will help reveal additional contextual factors that influence blind people's privacy concerns in the context of VAT use, e.g., camera form factor, image metadata, data regulations, whose personal data is captured in the image, the privacy protective practices VAT users enact at the micro or macro level to preserve their PVC, and remote visual assistants and technology developers adherence to personal data privacy and security measures), and investigate how these contextual factors affect users' privacy concerns for each PVC type and VAT type and condition. Moreover, additional research can be conducted to study the impact of ones' prior visual experience on ones' privacy concerns when using VATs, including whether the age at which a person lost their sight impacts their privacy concerns.

We believe it is important to assess these factors as independent variables as well as compounding. Potential future work includes a Contextual Integrity Analysis [76] to holistically evaluate how current VAT practices adhere to what VAT users deem appropriate, e.g., as having "contextual integrity", and how different privacy protective features introduce new norms, and/or change information flows to reduce the types of threats blind people deem to be negatively impacting their ability to get equitable access to information. We hypothesize that a structured Contextual Integrity Analysis will serve as a useful tool to evaluate how our findings from VAT users compare with the concerns of personal visual data sharing that occurs for different applications by

[15]The readability issues we observed include: (1) unclear subject headings; (2) inconsistent document structure (across all of the policies in our sample); (3) use of imprecise language to indicate which types of data are collected and length of data retention; (4) use of different terminology throughout the policies when referring to data (e.g., stating 'data' at the onset of the policy, personal information in another location, and content in another); (5) inclusion of information about use of data in sections related to the dissemination of data to third parties; and (6) reliance on the reader to have in-depth familiarity of the privacy policy to execute their choices.

the general public. Moreover, running fractal factorial vignette studies, e.g., [11] may be useful for determining the weight of various contextual factors VAT users' privacy preferences.

6.5.3 Applying Findings to Other Camera-Based Technologies and their Users. Finally, many other types of companies employ camera-based technologies (e.g., life-logging devices, robots, drones, and self-driving vehicles) to collect and process users' personal visual data. Given the growing collection of images and videos, the absolute number of privacy disclosures is expected to increase. Our research methods may be valuable for formative research into the visual data handling practices of companies that provide other camera-based services.

7 CONCLUSION

We conducted two independent but complementary studies to examine the privacy concerns that blind people have in the context of using VATs. Our empirical investigation into the factors that blind people identify as impacting their privacy in the context of their use of VATs, and the types of visual content blind people consider to be private in the context of their use of human- and AI-powered VATs reveal a suite of factors that benefit one's sense of privacy and factors that add risk to one's sense of privacy. Our analysis of the privacy policies of 13 VAT companies to understand what they communicate to VAT users about the collection and processing of personal visual data revealed that VAT companies did little to provide notice about the handling of users' visual data in their privacy policies. We offer our findings to help guide the development of privacy-protective VATs that address users' privacy concerns and empower users to decide which VATs to use based on alignment with their personal visual data privacy preferences. These recommendations center on (1) conducting user-centered research to design non-visual tools that provide users with the information necessary to provide informed consent for others to only access their images for visual assistance; (2) developing policies and functional safeguards that are specific to, at least, the type agent providing visual assistance (human or AI) and the types of private visual content in an image or video; and (3) embarking on designing new VATs based on the paradigm of "Privacy by Design" and evaluating them according to how they align with user's values.

8 SUPPLEMENTARY MATERIALS

8.1 Interview Protocol

Here we present the full version of our interview protocol. The protocol is organized to questions about the participants' backgrounds and Demographics, Semi-Structured questions about their use of **visual assistance technologies (VATs)** and privacy considerations in different situations, and the Ranking Activity.

8.1.1 Demographics.

(1) What is your Name?
(2) How old are you?
(3) What is the highest level of education you completed?
(4) What is your primary occupation?
(5) Level of vision- A) Totally blind, B) Legally blind, C) Low vision
(6) What is the medical diagnosis of your primary visual impairment?
(7) What is the medical diagnosis of your secondary visual impairment?
(8) At what age did you become [A) Totally blind, B) Legally blind, C) Low vision]
(9) What is your zip code?
(10) What is the primary access technology you use and what do you use it for?
(11) What is the secondary access technology you use and what do you use it for?

8.1.2 *Semi-Structured Questions.*

(1) What technology or device do you currently use to get information about your surroundings?
(2) What do you use [the technology...up to 3] for?
(3) What kind of information do you usually want from [the technology]?
(4) Can you describe how the VATs works to provide the information you want?
(5) What is usually in the photos or video you share with VATs?
(6) How many days a week do you use VATs?
(7) How much time each day do you spend using VATs?
(8) Are there any technologies that you would like to use, but have not yet tried?
(9) What features of that technology are appealing to you?
(10) What has prevented you from using [the technology]?
(11) What privacy concerns do you have in your everyday life?
(12) What information do you consider to be "private"?
(13) How do your privacy concerns impact your use of [the technology]?
(14) Sometimes people with visual impairments get the information they want about visual content from a real person, other times they get the information from an automated system. Do you have a preference for one or the other? Follow Up: What factors affect this choice? Follow Up: What factors influence your trust in these situations? Follow Up: Do you have any privacy concerns about these situations?
(15) When you share images or videos to get assistance, what content do you consider to be private?
(16) Why do you consider these content areas to be private?
(17) How do you know whether a picture or video you share via [the technologies] contains any private information?
(18) Now that we have talked about this, are there other privacy-related concerns or situations that are relevant to you in your everyday life?

8.1.3 *Ranking Questions.*

(1) Imagine that [X PVD] was available for anybody to use. How would that make you feel? In what situations would it be of particular concern to you?
(2) Rank your level of concern if you shared [the following private information] to Human-powered image description service Knowingly, and please provide your reason why;
(3) Rank your level of concern if you shared [the following private information] to Human-powered image description service Unknowingly, and please provide your reason why;
(4) Rank your level of concern if you shared [the following private information] to AI-powered image description service Knowingly, and please provide your reason why;
(5) Rank your level of concern if you shared [the following private information] to AI-powered image description service Unknowingly, and please provide your reason why.

Ranking Scores

(1) Not Concerned, i.e. Doesn't faze me;
(2) Mildly Concerned, i.e. I would think about it after the fact;
(3) Concerned, i.e. I would discuss it with other people;
(4) Very Concerned, i.e. I would develop strategies to change my behavior;
(5) Extremely Concerned, i.e. I would change my behavior immediately.

PVD Content Types Applied

- Picture where a face is visible/ Reflection of a face in a mirror or glass
- Picture of a naked body
- Framed photo of people
- Picture of a tattoo
- Pregnancy test result
- Pill bottle with a name, medical information, or address on it
- Letter with an address or name on it
- Business card with contact information on it
- Newspaper with the name of a city shown
- Receipt from a store showing a local address
- Miscellaneous papers with a name or local address visible
- Computer screen showing a username
- License plate number
- A local street sign
- A library book with a local branch's name on it
- Clothing with a logo of a company, organization, or group you affiliate with
- Location
- Name
- Address
- Medical information
- Financial account information
- Other/Emergent

9 CODE DEFINITIONS SHEET

Here we present the codes we applied to the data we analyzed.

Table 9. Code Sheet with Definitions

ID	Subcode or Subsubcode	Definition	Semi-Structured	
			Human-powered VATs	*AI-powered VATs*
1	**Information Designation**	**Instances when participants respond by indicating conditions that characterize the information**		
1.1	Public Information	Assessment that the information is easily accessed through a basic web search or is already available for the masses		
1.2	Needed Information	Assessment that they are compelled to get information to achieve task, knowingly shared-personal choice		
1.3	Content Dependent	Assessment that their response would vary based on the specific content of the image		
1.4	If Paired with Other Information/Metadata	Assessment that their response would vary based on whether one type of information was paired with another type of information		

(Continued)

Table 9. Continued

ID	Subcode or Subsubcode	Definition	Semi-Structured	
			Human-powered VATs	*AI-powered VATs*
2	**Sharing Choices**	**Instances when participants indicated something about the nature of the type of information**		
2.1	Common Practice	Assessment that they engage in the activity regularly		
2.2	Wouldn't Share Intentionally	Assessment that the introduced situation is outside of their realm of desired behavior		
3	**Personal/Social Impacts**	**Instances when participants make assessments about how the VATs' strategies influence their personal or their community's sense of well-being.**		
3.1	No Privacy Risks	Assessment that there is no impact		
3.2	No Risk of Identification	Assessment that the their identity would be safe regardless of disclosure of information		
3.3	Undefined Threat/ Consequence	Assessment that there is a risk with disclosure of information but unarticulated impact of that threat		
3.4	Unwanted Identity Disclosure	Assessment that the something about them will be revealed against their desires		
3.5	Identity Theft	Assessment that another person would use their information to impersonate them	Risk	
3.6	Financial Theft	Assessment that another person would use their information to deplete monetary resources		
3.7	Unwanted Identification of Location	Assessment that another person would use their information to find where they reside		
3.8	Unwanted Human Viewing	Risk that a person is looking at their information without their permission		
3.9	Social Judgement	Assessment that disclosure of information (or a certain behavior) would entice a negative critique from others, causing personal embarrassment or other psychological impact	Risk	Benefit
3.10	Damage to Reputation	Assessment that disclosure of information could impact the ways others perceive them and in turn creating a barrier to personal, social, or professional success		
3.11	Reveals Intimate Personal Experience	Assessment that disclosure of information will expose something that they hold sacred to one's sense of personal or close family relations		
3.12	Against HIPAA	Assessment that disclosure of the information would violate existing privacy policies associated with medical information		
3.13	Consent Not Given	Assessment that one's choice to give permission has been ignored or violated		

(Continued)

Table 9. Continued

ID	Subcode or Subsubcode	Definition	Semi-Structured	
			Human-powered VATs	*AI-powered VATs*
3.14	Betrayal of Trust	Assessment that disclosure of information would violate one's confidence in the reliability of another		
3.15	Betrayal Personal Rights	Assessment that disclosure of information would violate their sense of justice regarding something that every human is entitled to		
3.16	Blind Justice	Assessment that the rights of people who are blind are in question		
3.17	Loss of Control or Agency	Assessment that disclosure of information will result in a lesser state of power in their lives		
3.18	Without Personal Awareness-Control	Assessment that something has occurred outside one's power or understanding		
3.19	Lack of Personal Management	Assessment that they did not organize their environment such that an image taken would lead to an unwanted disclosure		
3.20	Not Socially Acceptable	Assessment that disclosure of information would be a deviation from the social norm or directly affecting others	Risk	
3.21	Personal Responsibility to Manage Information	Assessment that they have an obligation to change or observe their behavior to reduce risk of inadvertently sharing information and risking disclosure of PVI		
3.22	Multi-party privacy breach	Assessment that sharing another persons PVC can cause harm and/or the need to augment their behavior to mitigate or eliminate risk for another.		
4	**Understanding of the Service Offering**	**Instances when participants makes an assessment of the the strategies or choices VATs use to deliver their services and/or protect users' privacy.**		
4.1	Desired Feature	Assessment that the technology includes a feature that they like		
4.2	Standard Service Offering	Assessment that the technology currently offers a feature or service		
4.3	Promised Confidentiality	Assessment that there is an agreement between the user and the provider that their information will not be disclosed		
4.4	Protected by Policy	Assessment that the VATs terms of service protects their rights as a customer/user		
4.5	Professionalism	Assessment that the VATs enact practices to maintain professional standing within industry or with their users	Benefit	
4.6	Trained Agents	Assessment that the VATs employ and prepare agents to meet their users' wants and needs	Benefit	

(Continued)

Table 9. Continued

ID	Subcode or Subsubcode	Definition	Semi-Structured	
			Human-powered VATs	*AI-powered VATs*
4.7	No Human Eyes On Data	Assessment that people never see their information first hand, and in turn do not expose them to other people's scrutiny or theft		Benefit
4.8	Anonymity	Assessment that they are one of many, hard to hone in on one's specific data points		Benefit
4.9	Data Only on Device	Assessment that the information shared is not uploaded to the cloud, where others may have access		
4.10	Computers Can't Blush	Assessment that Artificial Intelligence does not have emotion or does not judge		
4.11	Personal Data is Anonymized	Assessment that information that is collected about a person is stripped of anything that is personally identifiable		
4.12	Service Development	Assessment that by sharing their information they are improving how VATs meets customers needs now or in the future		Benefit
4.13	Corporate Messaging	Assessment that a company marketing provides accurate information about the service		
4.14	Choice to Opt Out	Assessment that there is the ability to opt out of having information retained is a benefit of the system.	Benefit	
4.15	No Human Assurance	Assessment that they do not get personalized, human interaction		
4.16	System Vulnerable	Assessment that one's information is at risk due to frailty of the VATs' technology or data management		Risk
4.17	Unwanted Use of Data to Train	Assessment related to a company's use of their information to improve the service		
4.18	Unknown Data Handling	Assessment that their lack of understanding of if/how VATs collect and process their data, as well as knowledge about available privacy protections and are in turn exposed to greater risk	Risk	Risk
4.19	Unfamiliar with Person	Assessment that they do not know the person they share the information with		
4.20	Grounds for Termination of Use	Assessment that their personal action would ban them from using the service again		
4.21	Trust of Human Decency	Assessment that they can rely on the integrity of people providing the service to have their best interests in mind	Benefit	
4.22	Accuracy	Assessment of the validity of information they received in response to a request.	Benefit	
4.23	Accountability	Assessment that one is responsible for the fulfilment of their obligations		Risk
4.24	Inaccuracy of Technology	Risk or assessment that the service does not produce descriptions with enough precision or the descriptions provided are misleading		

The columns labeled human-powered VATs and AI-powered VATs Semi-Structured Columns indicate what codes emerged during the semi-structured interviews. All other codes emerged during the ranking task.

ACKNOWLEDGMENTS

We would like to thank the anonymous reviewers for their thoughtful feedback, Jaxsen Day for piloting our interview protocol, and Pardis Emami-Naeini and Philip Doty for providing feedback on earlier drafts of this manuscript. We would also like to thank the National Federation of the Blind for distributing materials recruitment to their membership.

REFERENCES

[1] Dustin Adams and Sri Kurniawan. 2014. A blind-friendly photography application for smartphones. *ACM SIGACCESS Accessibility and Computing* 108 (Jan. 2014), 12–15. DOI:http://dx.doi.org/10.1145/2591357.2591358

[2] Shane Ahern, Dean Eckles, Nathaniel S. Good, Simon King, Mor Naaman, and Rahul Nair. 2007. Over-exposed?: Privacy patterns and considerations in online and mobile photo sharing. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 357–366.

[3] Tousif Ahmed. 2019. *Towards the Design of Wearable Assistive Technologies to Address the Privacy and Security Concerns of People with Visual Impairments*. PhD Thesis. Indiana University.

[4] 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 - CHI'15*. ACM Press, Seoul, Republic of Korea, 3523–3532. DOI:http://dx.doi.org/10.1145/2702123.2702334

[5] Tousif Ahmed, Patrick Shaffer, Kay Connelly, David Crandall, and Apu Kapadia. 2016. Addressing physical safety, security, and privacy for people with visual impairments. In *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)*. 341–354. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/ahmed.

[6] AIpoly. 2020. AIpoly Homepage. (2020). https://www.aipoly.com/.

[7] Aira. 2020. Aira. (2020). https://aira.io/. Library Catalog: aira.io.

[8] Taslima Akter. 2020. Privacy considerations of the visually impaired with camera based assistive tools. In *Conference Companion Publication of the 2020 on Computer Supported Cooperative Work and Social Computing*. ACM, Virtual Event USA, 69–74. DOI:http://dx.doi.org/10.1145/3406865.3418382

[9] Taslima Akter, Bryan Dosono, Tousif Ahmed, Apu Kapadia, and Bryan Semaan. 2020. "I am uncomfortable sharing what I can't see": Privacy concerns of the visually impaired with camera based assistive applications. In *29th {USENIX} Security Symposium ({USENIX} Security 20)*. https://www.usenix.org/conference/usenixsecurity20/presentation/akter.

[10] ACM ASSETS. 2019. 21st International ACM SIGACCESS Conference on Computers and Accessibility. (2019). https://assets19.sigaccess.org/.

[11] Christiane Atzmüller and Peter M. Steiner. 2010. Experimental vignette studies in survey research. *Methodology* (June 2010). https://econtent.hogrefe.com/doi/abs/10.1027/1614-2241/a000014. Publisher: Hogrefe Publishing.

[12] Cynthia L. Bennett, Jane E., Martez E. Mott, Edward Cutrell, and Meredith Ringel Morris. 2018. How teens with visual impairments take, edit, and share photos on social media. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, Montreal QC Canada, 1–12. DOI:http://dx.doi.org/10.1145/3173574.3173650

[13] Cynthia L. Bennett, Cole Gleason, Morgan Klaus Scheuerman, Jeffrey P. Bigham, Anhong Guo, and Alexandra To. 2021. "It's complicated": Negotiating accessibility and (mis)representation in image descriptions of race, gender, and disability. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI'21)*. Association for Computing Machinery, New York, NY, USA, 1–19. DOI:http://dx.doi.org/10.1145/3411764.3445498

[14] Andrew Besmer and Heather Lipford. 2009. Tagged photos: Concerns, perceptions, and protections. In *CHI'09 Extended Abstracts on Human Factors in Computing Systems*. ACM, 4585–4590.

[15] BeSpecular. 2020. BeSpecular. (2020). https://www.bespecular.com/.

[16] Hugh Beyer and Karen Holtzblatt. 1998. Contextual design: Defining customer-centered systems. 1998. *San Francisco: Morgan Kauffman* (1998).

[17] Jeffrey P. Bigham, Richard E. Ladner, and Yevgen Borodin. 2011. The design of human-powered access technology. In *The Proceedings of the 13th International ACM SIGACCESS Conference on Computers and Accessibility - ASSETS'11*. ACM Press, Dundee, Scotland, UK, 3. DOI:http://dx.doi.org/10.1145/2049536.2049540

[18] Jeffrey P. Bigham, Tom Yeh, Chandrika Jayant, Hanjie Ji, Greg Little, Andrew Miller, Robert C. Miller, Aubrey Tatarowicz, Brandyn White, and Samuel White. 2010. VizWiz: Nearly real-time answers to visual questions. In *Proceedings of the 2010 International Cross Disciplinary Conference on Web Accessibility (W4A) - W4A'10*. ACM Press, Raleigh, North Carolina, 1. DOI:http://dx.doi.org/10.1145/1805986.1806020

[19] Erin Brady, Meredith Ringel Morris, Yu Zhong, Samuel White, and Jeffrey P. Bigham. 2013. Visual challenges in the everyday lives of blind people. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI'13*. ACM Press, Paris, France, 2117. DOI:http://dx.doi.org/10.1145/2470654.2481291

[20] Erin Brady, Yu Zhong, and Jeffrey P. Bigham. 2015. Creating accessible PDFs for conference proceedings. In *Proceedings of the 12th Web for All Conference on - W4A'15*. ACM Press, Florence, Italy, 1–4. DOI:http://dx.doi.org/10.1145/2745555.2746665

[21] Stacy M. Branham, Ali Abdolrahmani, William Easley, Morgan Scheuerman, Erick Ronquillo, and Amy Hurst. 2017. "Is someone there? Do they have a gun": How visual information about others can improve personal safety management for blind individuals. In *Proceedings of the 19th International ACM SIGACCESS Conference on Computers and Accessibility*. ACM, Baltimore Maryland USA, 260–269. DOI:http://dx.doi.org/10.1145/3132525.3132534

[22] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (Jan. 2006), 77–101. DOI:http://dx.doi.org/10.1191/1478088706qp063oa

[23] Travis D. Breaux, Hanan Hibshi, and Ashwini Rao. 2014. Eddy, a formal language for specifying and analyzing data flow specifications for conflicting privacy requirements. *Requirements Engineering* 19, 3 (Sept. 2014), 281–307. DOI:http://dx.doi.org/10.1007/s00766-013-0190-7

[24] Shonal Chaudhry and Rohitash Chandra. 2015. Design of a mobile face recognition system for visually impaired persons. *arXiv preprint arXiv:1502.00756* (2015).

[25] Tai-Yin Chiu, Yinan Zhao, and Danna Gurari. 2020. Assessing image quality issues for real-world problems. In *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*. 3643–3653. DOI:http://dx.doi.org/10.1109/CVPR42600.2020.00370. ISSN: 2575-7075.

[26] Federal Trade Commission. 1998. Privacy Online: A Report to Congress. (June 1998), 71. https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

[27] Federal Trade Commission. 2000. Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress. (May 2000). https://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission.

[28] Federal Trade Commission. 2013. Children's Online Privacy Protection Act (COPPA). (July 2013). https://www.ftc.gov/enforcement/statutes/childrens-online-privacy-protection-act.

[29] Federal Trade Commission. 2018. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act). (Nov. 2018). https://www.ftc.gov/enforcement/statutes/controlling-assault-non-solicited-pornography-marketing-act-2003-can-spam-act.

[30] Federal Trade Commission. 2020. Gramm-Leach-Bliley Act. (2020). https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act. Library Catalog: www.ftc.gov.

[31] Ned Desmond. 2020a. Microsoft's Seeing AI founder Saqib Shaikh is speaking at Sight Tech Global. (2020). https://social.techcrunch.com/2020/08/20/microsofts-seeing-ai-founder-saqib-shaikh-is-speaking-at-sight-tech-global/.

[32] Ned Desmond. 2020b. Sight Tech Global - Shaping New Technologies to Create a More Accessible World for People with Blindness and Visual Impairments. (2020). https://sighttechglobal.com/.

[33] European Commission. 2018. EU data protection rules. (2018). https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en.

[34] Be My Eyes. 2020. Be My Eyes - See the world together. (2020). https://www.bemyeyes.com/. Library Catalog: www.bemyeyes.com.

[35] Kenneth R. Fleischmann. 2013. Information and human values. *Synthesis Lectures on Information Concepts, Retrieval, and Services* 5, 5 (Nov. 2013), 1–99. DOI:http://dx.doi.org/10.2200/S00545ED1V01Y201310ICR031 Publisher: Morgan & Claypool Publishers.

[36] Computer Vision Foundation. 2019. Conference on Computer Vision and Pattern Recognition 2019. (2019). http://cvpr2019.thecvf.com/.

[37] Batya Friedman, Peter H. Kahn, and Alan Borning. 2008. Value sensitive design and information systems. *The Handbook of Information and Computer Ethics* (2008), 69–101. Publisher: Wiley Online Library.

[38] Andrea Frome, German Cheung, Ahmad Abdulkader, Marco Zennaro, Bo Wu, Alessandro Bissacco, Hartwig Adam, Hartmut Neven, and Luc Vincent. 2009. Large-scale privacy protection in Google Street View. In *2009 IEEE 12th International Conference on Computer Vision*. IEEE, 2373–2380.

[39] Lisa Given. 2008. *The SAGE Encyclopedia of Qualitative Research Methods*. SAGE Publications, Inc. DOI:http://dx.doi.org/10.4135/9781412963909

[40] Cole Gleason, Patrick Carrington, Lydia B. Chilton, Benjamin M. Gorman, Hernisa Kacorri, Andrés Monroy-Hernández, Meredith Ringel Morris, Garreth W. Tigwell, and Shaomei Wu. 2019. Addressing the accessibility of social media. In *Conference Companion Publication of the 2019 on Computer Supported Cooperative Work and Social Computing*. ACM, Austin TX USA, 474–479. DOI:http://dx.doi.org/10.1145/3311957.3359439

[41] Cole Gleason, Amy Pavel, Himalini Gururaj, Kris Kitani, and Jeffrey Bigham. 2020. Making GIFs accessible. In *The 22nd International ACM SIGACCESS Conference on Computers and Accessibility*. ACM, Virtual Event Greece, 1–10. DOI:http://dx.doi.org/10.1145/3373625.3417027

[42] Cole Gleason, Amy Pavel, Xingyu Liu, Patrick Carrington, Lydia B. Chilton, and Jeffrey P. Bigham. 2019. Making memes accessible. In *The 21st International ACM SIGACCESS Conference on Computers and Accessibility*. ACM, Pittsburgh PA USA, 367–376. DOI:http://dx.doi.org/10.1145/3308561.3353792

[43] Cole Gleason, Amy Pavel, Emma McCamey, Christina Low, Patrick Carrington, Kris M. Kitani, and Jeffrey P. Bigham. 2020. Twitter a11y: A browser extension to make Twitter images accessible. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, Honolulu HI USA, 1–12. DOI:http://dx.doi.org/10.1145/3313831.3376728

[44] Danna Gurari and Kristen Grauman. 2017. CrowdVerge: Predicting if people will agree on the answer to a visual question. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, Denver Colorado USA, 3511–3522. DOI:http://dx.doi.org/10.1145/3025453.3025781

[45] Danna Gurari, Qing Li, Chi Lin, Yinan Zhao, Anhong Guo, Abigale Stangl, and Jeffrey P. Bigham. 2019. VizWiz-Priv: A dataset for recognizing the presence and purpose of private visual information in images taken by blind people. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. 939–948.

[46] Danna Gurari, Qing Li, Abigale J. Stangl, Anhong Guo, Chi Lin, Kristen Grauman, Jiebo Luo, and Jeffrey P. Bigham. 2018. VizWiz grand challenge: Answering visual questions from blind people. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. 3608–3617.

[47] Danna Gurari, Yinan Zhao, Meng Zhang, and Nilavra Bhattacharya. 2020. Captioning images taken by people who are blind. In *Computer Vision – ECCV 2020 (Lecture Notes in Computer Science)*, Andrea Vedaldi, Horst Bischof, Thomas Brox, and Jan-Michael Frahm (Eds.). Springer International Publishing, Cham, 417–434. DOI:http://dx.doi.org/10.1007/978-3-030-58520-4_25

[48] Hana Habib, Yixin Zou, Aditi Jannu, Neha Sridhar, Chelse Swoopes, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2019. An empirical analysis of data deletion and {Opt-Out} choices on 150 websites. 387–406. https://www.usenix.org/conference/soups2019/presentation/habib.

[49] Gene E. Hall et al. 1977. *Measuring Stages of Concern About the Innovation: A Manual for the Use of the SoC Questionnaire*. https://eric.ed.gov/?id=ED147342.

[50] Hamza Harkous, Kassem Fawaz, Rémi Lebret, Florian Schaub, Kang G. Shin, and Karl Aberer. 2018. Polisis: Automated analysis and presentation of privacy policies using deep learning. In *27th {USENIX} Security Symposium ({USENIX} Security 18)*. 531–548. https://www.usenix.org/conference/usenixsecurity18/presentation/harkous.

[51] Jordan Hayes, Smirity Kaushik, Charlotte Emily Price, and Yang Wang. 2019. Cooperative privacy and security: Learning from people with visual impairments and their allies. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS) 2019*.

[52] Candice Hoke, Lorrie Cranor, Pedro Leon, and Alyssa Au. 2015. Are they worth reading? An in-depth analysis of online trackers' privacy policies. *I/S: A Journal of Law and Policy for the Information Society* (April 2015). https://engagedscholarship.csuohio.edu/fac_articles/783.

[53] Roberto Hoyle, Luke Stark, Qatrunnada Ismail, David Crandall, Apu Kapadia, and Denise Anthony. 2020. Privacy norms and preferences for photos posted online. *ACM Transactions on Computer-Human Interaction* 27, 4 (Sept. 2020), 1–27. DOI:http://dx.doi.org/10.1145/3380960

[54] AI Now Institute. 2019. *Disability, Bias, and AI*. https://ainowinstitute.org/disabilitybiasai-2019.pdf.

[55] Rabia Jafri, Syed Abid Ali, and Hamid R. Arabnia. 2013. Face recognition for the visually impaired. In *Proceedings of the International Conference on Information and Knowledge Engineering (IKE)*. The Steering Committee of The World Congress in Computer Science, Computer, 1.

[56] Chandrika Jayant, Hanjie Ji, Samuel White, and Jeffrey P. Bigham. 2011. Supporting blind photography. In *The Proceedings of the 13th International ACM SIGACCESS Conference on Computers and Accessibility - ASSETS'11*. ACM Press, Dundee, Scotland, UK, 203. DOI:http://dx.doi.org/10.1145/2049536.2049573

[57] 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, Vienna, Austria, 471–478. DOI:http://dx.doi.org/10.1145/985692.985752

[58] Shaun K. Kane, Chandrika Jayant, Jacob O. Wobbrock, and Richard E. Ladner. 2009. Freedom to roam: A study of mobile device adoption and accessibility for people with visual and motor disabilities. In *Proceeding of the Eleventh International ACM SIGACCESS Conference on Computers and Accessibility - ASSETS'09*. ACM Press, Pittsburgh, Pennsylvania, USA, 115. DOI:http://dx.doi.org/10.1145/1639642.1639663

[59] 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 28th International Conference on Human Factors in Computing Systems - CHI'10*. ACM Press, Atlanta, Georgia, USA, 1573. DOI:http://dx.doi.org/10.1145/1753326.1753561

[60] KNFB Reader. 2020. App features the best OCR. Turns print into speech or Braille instantly. iOS 3 now available. | KNFB Reader. (2020). https://knfbreader.com/.

[61] K. M. Kramer, D. S. Hedin, and D. J. Rolkosky. 2010. Smartphone based face recognition tool for the blind. In *2010 Annual International Conference of the IEEE Engineering in Medicine and Biology*. IEEE, 4538–4541.

[62] Barbara Krumay and Jennifer Klar. 2020. Readability of privacy policies. In *Data and Applications Security and Privacy XXXIV (Lecture Notes in Computer Science)*, Anoop Singhal and Jaideep Vaidya (Eds.). Springer International Publishing, Cham, 388–399. DOI:http://dx.doi.org/10.1007/978-3-030-49669-2_22

[63] Kyungjun Lee, Daisuke Sato, Saki Asakawa, Hernisa Kacorri, and Chieko Asakawa. 2020b. Pedestrian detection with wearable cameras for the blind: A two-way perspective. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI'20)*. Association for Computing Machinery, New York, NY, USA, 112. DOI:http://dx.doi.org/10.1145/3313831.3376398 event-place: Honolulu, HI, USA.

[64] Sooyeon Lee, Madison Reddie, Chun-Hua Tsai, Jordan Beck, Mary Beth Rosson, and John M. Carroll. 2020a. The emerging professional practice of remote sighted assistance for people with visual impairments. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, Honolulu HI USA, 1–12. DOI:http://dx.doi.org/10.1145/3313831.3376591

[65] Na Li, Maryam Najafian Razavi, and Denis Gillet. 2011. Trust-aware privacy control for social media. In *CHI'11 Extended Abstracts on Human Factors in Computing Systems (CHI EA'11)*. Association for Computing Machinery, Vancouver, BC, Canada, 1597–1602. DOI:http://dx.doi.org/10.1145/1979742.1979814

[66] Yifang Li, Nishant Vishwamitra, Hongxin Hu, and Kelly Caine. 2020. Towards a taxonomy of content sensitivity and sharing preferences for photos. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, Honolulu HI USA, 1–14. DOI:http://dx.doi.org/10.1145/3313831.3376498

[67] Thomas Linden, Rishabh Khandelwal, Hamza Harkous, and Kassem Fawaz. 2020. The privacy policy landscape after the GDPR. *Proceedings on Privacy Enhancing Technologies* 2020, 1 (Jan. 2020), 47–64. DOI:http://dx.doi.org/10.2478/popets-2020-0004

[68] Heather Richter Lipford, Jason Watson, Michael Whitney, Katherine Froiland, and Robert W. Reeder. 2010. Visual vs. compact: A comparison of privacy policy interfaces. In *Proceedings of the 28th International Conference on Human Factors in Computing Systems - CHI'10*. ACM Press, Atlanta, Georgia, USA, 1111. DOI:http://dx.doi.org/10.1145/1753326.1753492

[69] LookTel. 2020. *Instant Recognition Apps for Persons with Low Vision or Blindness*. http://www.looktel.com/.

[70] Haley MacLeod, Cynthia L. Bennett, Meredith Ringel Morris, and Edward Cutrell. 2017. Understanding blind people's experiences with computer-generated captions of social media images. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, Denver Colorado USA, 5988–5999. DOI:http://dx.doi.org/10.1145/3025453.3025814

[71] Aleecia M. McDonald and Lorrie Faith Cranor. 2008. The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society* 4 (2008), 543. Publisher: HeinOnline.

[72] Nora McDonald and Andrea Forte. 2020. The politics of privacy theories: Moving from norms to vulnerabilities. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, Honolulu HI USA, 1–14. DOI:http://dx.doi.org/10.1145/3313831.3376167

[73] Gabriele Meiselwitz. 2013. Readability assessment of policies and procedures of social networking sites. In *Online Communities and Social Computing (Lecture Notes in Computer Science)*, A. Ant Ozok and Panayiotis Zaphiris (Eds.). Springer, Berlin, 67–75. DOI:http://dx.doi.org/10.1007/978-3-642-39371-6_8

[74] Microsoft. 2020. Seeing AI App from Microsoft. (2020). https://www.microsoft.com/en-us/ai/seeing-ai. Library Catalog: www.microsoft.com.

[75] Meredith Ringel Morris. 2019. AI and accessibility: A discussion of ethical considerations. *arXiv:1908.08939 [cs]* (Aug. 2019). http://arxiv.org/abs/1908.08939.

[76] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Washington Law Review* 79 (2004), 41.

[77] State of California Department of Justice. 2018. California Consumer Privacy Act (CCPA). (Oct. 2018). https://oag.ca.gov/privacy/ccpa.

[78] OrCam. 2020. *Never Forget a Face*. https://myme.orcam.com/.

[79] Tribhuvanesh Orekondy, Bernt Schiele, and Mario Fritz. 2017. Towards a visual privacy advisor: Understanding and predicting privacy risks in images. In *2017 IEEE International Conference on Computer Vision (ICCV)*. IEEE, Venice, 3706–3715. DOI:http://dx.doi.org/10.1109/ICCV.2017.398

[80] European Parliament and Council of European Union. 2016. *General Data Protection Regulation (GDPR) Compliance Guidelines*. https://gdpr.eu/.

[81] Sören Preibusch. 2013. Guide to measuring privacy concern: Review of survey and observational instruments. *International Journal of Human-Computer Studies* 71, 12 (Dec. 2013), 1133–1143. DOI:http://dx.doi.org/10.1016/j.ijhcs.2013.09.002

[82] Rohan Ramanath, Fei Liu, Norman Sadeh, and Noah A. Smith. 2014. Unsupervised alignment of privacy policies using hidden Markov models. In *Proceedings of the 52nd Annual Meeting of the Association for Computational Linguistics*

(Volume 2: Short Papers). Association for Computational Linguistics, Baltimore, Maryland, 605–610. DOI:http://dx.doi.org/10.3115/v1/P14-2099

[83] Looktel Money Reader. 2020. *LookTel Money Reader for iPhone, iPod Touch and Mac*. http://www.looktel.com/moneyreader.

[84] Joel R. Reidenberg, Travis Breaux, Lorrie Faith Cranor, Brian French, Amanda Grannis, James T. Graves, Fei Liu, Aleecia McDonald, Thomas B. Norton, and Rohan Ramanath. 2015. Disagreeable privacy policies: Mismatches between meaning and users' understanding. *Berkeley Technology Law Journal* 30, 1 (2015), 1–88. https://heinonline.org/HOL/P?h=hein.journals/berktech30&i=51.

[85] Joel R. Reidenberg, N. Cameron Russell, Alexander Callen, Sophia Qasir, and Thomas Norton. 2014. Privacy harms and the effectiveness of the notice and choice framework. *SSRN Electronic Journal* (2014). DOI:http://dx.doi.org/10.2139/ssrn.2418247

[86] Manuel Rudolph, Denis Feth, and Svenja Polst. 2018. Why users ignore privacy policies–a survey and intention model for explaining user privacy behavior. In *International Conference on Human-Computer Interaction*. Springer, 587–598.

[87] Florian Schaub, Rebecca Balebako, and Lorrie Faith Cranor. 2017. Designing effective privacy notices and controls. *IEEE Internet Computing* (2017), 1–1. DOI:http://dx.doi.org/10.1109/MIC.2017.265102930

[88] Shalom H. Schwartz. 1994. Are there universal aspects in the structure and contents of human values? *Journal of Social Issues* 50, 4 (1994), 19–45. Publisher: Wiley Online Library.

[89] Kristen Shinohara and Jacob O. Wobbrock. 2011. In the shadow of misperception: Assistive technology use and social interactions. In *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems - CHI'11*. ACM Press, Vancouver, BC, Canada, 705. DOI:http://dx.doi.org/10.1145/1978942.1979044

[90] Rachel N. Simons, Danna Gurari, and Kenneth R. Fleischmann. 2020. "I hope this is helpful": Understanding crowdworkers' challenges and motivations for an image description task. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2 (Oct. 2020), 1–26. DOI:http://dx.doi.org/10.1145/3415176

[91] R. I. Singh, M. Sumeeth, and J. Miller. 2011. Evaluating the readability of privacy policies in mobile environments. *International Journal of Mobile Human Computer Interaction* 3, 1 (Jan. 2011), 55–78. DOI:http://dx.doi.org/10.4018/jmhci.2011010104

[92] H. Jeff Smith, Sandra J. Milberg, and Sandra J. Burke. 1996. Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly* (1996), 167–196. Publisher: JSTOR.

[93] Anna C. Squicciarini, Cornelia Caragea, and Rahul Balakavi. 2014. Analyzing images' privacy for the modern web. In *Proceedings of the 25th ACM Conference on Hypertext and Social Media*. ACM, Santiago Chile, 136–147. DOI:http://dx.doi.org/10.1145/2631775.2631803

[94] Mukund Srinath, Shomir Wilson, and C. Lee Giles. 2020. Privacy at scale: Introducing the PrivaSeer corpus of web privacy policies. *arXiv:2004.11131 [cs]* (April 2020). http://arxiv.org/abs/2004.11131. arXiv: 2004.11131.

[95] Abigale Stangl, Meredith Ringel Morris, and Danna Gurari. 2020a. "Person, shoes, tree. Is the person naked?" What people with vision impairments want in image descriptions. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI'20)*. Association for Computing Machinery, Honolulu, HI, USA, 1–13. DOI:http://dx.doi.org/10.1145/3313831.3376404

[96] Abigale Stangl, Kristina Shiroma, Bo Xie, Kenneth R. Fleischmann, and Danna Gurari. 2020b. Visual content considered private by people who are blind. In *The 22nd International ACM SIGACCESS Conference on Computers and Accessibility*. ACM, Virtual Event Greece, 1–12. DOI:http://dx.doi.org/10.1145/3373625.3417014

[97] Anselm L. Strauss. 1987. *Qualitative Analysis for Social Scientists*. Cambridge University Press.

[98] Madiha Tabassum, Abdulmajeed Alqhatani, Marran Aldossari, and Heather Richter Lipford. 2018. Increasing user attention with a comic-based policy. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, Montreal QC Canada, 1–6. DOI:http://dx.doi.org/10.1145/3173574.3173774

[99] TapTapSee. 2020. *Blind and Visually Impaired Assistive Technology - powered by CloudSight.ai Image Recognition API*. https://taptapseeapp.com/.

[100] Eran Toch, Norman M. Sadeh, and Jason Hong. 2010. Generating default privacy policies for online social networks. In *Proceedings of the 28th International Conference Extended Abstracts on Human Factors in Computing Systems - CHI EA'10*. ACM Press, Atlanta, Georgia, USA, 4243. DOI:http://dx.doi.org/10.1145/1753846.1754133

[101] Education United States. Department of Health and Welfare Office for Civil Rights. 1973. Section 504 Of the Rehabilitation Act of 1973: Fact Sheet : Handicapped Persons Rights under Federal Law. (1973).

[102] Yang Wang. 2017. The third wave? Inclusive privacy and security. In *Proceedings of the 2017 New Security Paradigms Workshop (NSPW 2017)*. Association for Computing Machinery, New York, NY, USA, 122–130. DOI:http://dx.doi.org/10.1145/3171533.3171538

[103] Yang Wang, Liang Gou, Anbang Xu, Michelle X. Zhou, Huahai Yang, and Hernan Badenes. 2015. VeilMe: An interactive visualization tool for privacy configuration of using personality traits. In *Proceedings of the 33rd Annual*

ACM Conference on Human Factors in Computing Systems. ACM, Seoul, Republic of Korea, 817–826. DOI:http://dx.doi.org/10.1145/2702123.2702293

[104] Richard Warner. 2020. *Notice and Choice Must Go: The Collective Control Alternative*. SSRN Scholarly Paper ID 3566630. Social Science Research Network, Rochester, NY. DOI:http://dx.doi.org/10.2139/ssrn.3566630

[105] Samuel D. Warren and Louis D. Brandeis. 1890. The right to privacy. *Harvard Law Review* 4, 5 (1890), 193–220. DOI:http://dx.doi.org/10.2307/1321160. Publisher: The Harvard Law Review Association.

[106] Shomir Wilson, Florian Schaub, 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 Reidenberg, and Norman Sadeh. 2016. The creation and analysis of a website privacy policy corpus. In *Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*. Association for Computational Linguistics, Berlin, Germany, 1330–1340. DOI:http://dx.doi.org/10.18653/v1/P16-1126

[107] Richmond Y. Wong and Deirdre K. Mulligan. 2019. Bringing design to the privacy table: Broadening "Design" in "privacy by design" through the lens of HCI. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI'19)*. Association for Computing Machinery, New York, NY, USA, 1–17. DOI:http://dx.doi.org/10.1145/3290605.3300492

[108] 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* 18, 4 (Nov. 2018), 1–18. DOI:http://dx.doi.org/10.1145/3127519

[109] Sergej Zerr, Stefan Siersdorfer, and Jonathon Hare. 2012. PicAlert!: A system for privacy-aware image classification and retrieval. In *Proceedings of the 21st ACM International Conference on Information and Knowledge Management*. ACM, 2710–2712.

[110] Yu Zhong, Walter S. Lasecki, Erin Brady, and Jeffrey P. Bigham. 2015. RegionSpeak: Quick comprehensive spatial descriptions of complex images for blind users. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI'15*. ACM Press, Seoul, Republic of Korea, 2353–2362. DOI:http://dx.doi.org/10.1145/2702123.2702437

[111] Sebastian Zimmeck, Peter Story, Daniel Smullen, Abhilasha Ravichander, Ziqi Wang, Joel Reidenberg, N. Cameron Russell, and Norman Sadeh. 2019. MAPS: Scaling privacy compliance analysis to a million apps. *Proceedings on Privacy Enhancing Technologies* 2019, 3 (July 2019), 66–86. DOI:http://dx.doi.org/10.2478/popets-2019-0037

[112] Sebastian Zimmeck, Ziqi Wang, Lieyong Zou, Roger Iyengar, Bin Liu, Florian Schaub, Shomir Wilson, Norman Sadeh, Steven M. Bellovin, and Joel Reidenberg. 2017. Automated analysis of privacy requirements for mobile apps. In *Proceedings 2017 Network and Distributed System Security Symposium*. Internet Society, San Diego, CA. DOI:http://dx.doi.org/10.14722/ndss.2017.23034

[113] California State University, Center on Disabilities and Northridge. 34th CSUN Assistive Technology Conference. Retrieved on 14 Oct., 2020 https://www.csun.edu/cod/conference.

Received June 2021; revised January 2022; accepted February 2022