

# Visual Content Considered Private by People Who are Blind

Abigale Stangl  
University of Texas at Austin  
Austin, Texas  
stangl@utexas.edu

Kristina Shiroma  
University of Texas at Austin  
Austin, Texas  
kristinashiroma@utexas.edu

Bo Xie  
University of Texas at Austin  
Austin, Texas  
boxie@utexas.edu

Kenneth R. Fleischmann  
University of Texas at Austin  
Austin, Texas  
kfleisch@utexas.edu

Danna Gurari  
University of Texas at Austin  
Austin, Texas  
danna.gurari@ischool.utexas.edu

## ABSTRACT

We present an empirical study into the visual content people who are blind consider to be private. We conduct a two-stage interview with 18 participants that identifies what they deem private in general and with respect to their use of services that describe their visual surroundings based on camera feeds from their personal devices. We then describe a taxonomy of private visual content that is reflective of our participants' privacy-related concerns and values. We discuss how this taxonomy can benefit services that collect and sell visual data containing private information so such services are better aligned with their users.

## CCS CONCEPTS

• **Human-centered computing** → **Empirical studies in accessibility**.

## KEYWORDS

privacy, visual data, private visual content, visual interpretation, image description, computer vision, people who are blind

### ACM Reference Format:

Abigale Stangl, Kristina Shiroma, Bo Xie, Kenneth R. Fleischmann, and Danna Gurari. 2020. Visual Content Considered Private by People Who are Blind. In *The 22nd International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS '20)*, October 26–28, 2020, Virtual Event, Greece. ACM, New York, NY, USA, 12 pages. <https://doi.org/10.1145/3373625.3417014>

## 1 INTRODUCTION

Many people who are blind<sup>1</sup> share images and videos they take with *Visual Interpreters or Description Services (VIDS)*, such as Seeing AI, Aira, Be My Eyes, TapTapSee, and Be Specular. VIDS enable users to receive descriptions of the visual media they share. With

<sup>1</sup>Throughout this paper we use people-first language, except when the grammatical structure of the sentence required otherwise. We also acknowledge that different people have different preferences for how they identify their visual impairment.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from [permissions@acm.org](https://permissions.acm.org).

*ASSETS '20*, October 26–28, 2020, Virtual Event, Greece

© 2020 Association for Computing Machinery.

ACM ISBN 978-1-4503-7103-2/20/10...\$15.00

<https://doi.org/10.1145/3373625.3417014>

such services, users can share camera feeds from their personal devices in order to receive descriptions of their visual surroundings, which in turn empowers them to more easily accomplish a variety of everyday tasks including shopping, cooking, reading mail, determining what to wear, and navigation (orientation and mobility) [8–10, 16, 18, 28, 39, 53, 64, 65].

Currently, little is understood about the privacy concerns of people who are blind in the context of their VIDS use, despite the facts that: (A) people who are blind take images that contain content that may be considered private and share them with VIDS, knowingly or unknowingly [36], (B) people who are blind are concerned about their privacy in their everyday environments and when using technology [1, 6, 7, 12–14, 22, 24, 27, 38, 43, 48, 52, 67], and (C) privacy is a core value implicated in system design [31].

Accordingly, we offer a systematic analysis to define the types of visual information people who are blind consider to be private, an endeavor we believe important for the development of VIDS and their privacy controls. Towards this aim, we present findings from 18 interviews with people who are blind during which we investigated the types of image content they consider to be private, as well as the underlying factors that influence their sense of privacy when using VIDS. We refer to private information in images/videos as *Private Visual Content (PVC)*. We used this analysis to prioritize which types of privacy content leaks are of greater/lesser concern.

Our investigation acknowledges the nuance that VIDS can employ either human agents and/or computer vision algorithms—a type of artificial intelligence (AI)—to describe images. Recently, prior work noted that the visual information sharing preferences and privacy concerns of people who are blind can vary based on the types of VIDS they use [11]. Our work provides concrete guidance in support of this claim by identifying privacy concerns separately for the contexts of Human-powered VIDS (*H-VIDS*) and AI-powered VIDS (*AI-VIDS*). We further enrich this analysis by identifying how people's privacy concerns are affected based on whether they knowingly versus inadvertently share private data with H-VIDS or AI-VIDS.

More generally, our findings can be used by developers to create PVC-aware VIDS that mitigate the privacy risks that their use entails. Our work serves as a valuable foundation for the development of user-centered privacy protections in VIDS that address the recent calls to “*protect people who fall outside of the ‘norms’ reflected and constructed by AI systems*” [40] and to develop AI systems based

in ethical considerations [50, 66]. We expect incorporating the perspectives of people who are blind on PVC can benefit society at large in accessing PVC-aware vision technology.

## 2 BACKGROUND AND RELATED WORK

In this section, we first provide background information on VIDS. We then discuss our current understanding about how people who are blind use VIDS, known privacy concerns of people who are blind, and prior efforts to develop taxonomies defining what is private visual content.

### 2.1 Visual Interpreters or Description Services

Over the past decade, a variety of visual interpreters or description services (VIDS) have been developed to provide users with descriptions of their visual surroundings. There are two common types. One type entails captioning, by taking as input visual content and returning a description of the content such as colors, text, money, objects, and people [2, 8, 9, 25, 28, 41, 44, 49, 55, 57, 64]. The other type entails visual question answering, and takes as input both visual content and a question about the visual content and then returns an answer [10, 16, 18]. In this paper, we focus on VIDS of both types that center on users submitting their own visual content.

VIDS are often characterized by the kind of agents that provide the descriptions of the visual content. Human-powered VIDS (H-VIDS) [19] rely on humans, including crowd workers [69], friends [21], social microvolunteers [20], and trained professionals [10]. AI-powered VIDS (AI-VIDS) instead rely on computer vision models. In this paper, we draw on the distinction between H-VIDS and AI-VIDS, based on evidence that the privacy concerns of people who are blind vary when obtaining descriptions from different types of agents [11, 38]. To the best of our knowledge, our work is the first published effort to decipher how the privacy concerns of people who are blind might differ based on whether users employ H-VIDS or AI-VIDS.

### 2.2 Understanding VIDS Use by People Who Are Blind and Have Low Vision

Prior work has sought to better understand how people who are blind use VIDS. Most prior work reports about general aspects of VIDS including the types of images and questions people who are blind share with VIDS [21, 26, 33–36] as well as the experiences of remote sighted assistants and the types of support remote sighted assistants offer [46]. Most related to our work is that of Akter et al. [11], who found from a survey with 155 people who are blind and have low vision that participants' concerns about privacy in the context of using VIDS shift according to (a) the kind of relationship they have with the person or services they share their visual information with, and (b) whether they are sharing images showing themselves versus others.

Our study extends prior work in two important ways. First, we identify what content people who are blind consider to be PVC in the context of VIDS use for a greater number of privacy types; i.e., we analyze 21 privacy types while Akter et al. only examine 5 types. Second, we examine how people's privacy concerns change when they share their private data knowingly versus inadvertently, given

that people who are blind both intentionally and inadvertently share information they consider to be private with VIDS [3, 34, 42].

### 2.3 Understanding Privacy Concerns of People Who Are Blind

Scholars have written extensively about the privacy, security, and safety concerns of people who are blind. Some studies focus on environmental factors [6, 7, 22, 38], while others examine use of mobile technologies and wearable devices [5, 13, 27, 43, 45, 52, 60]. Findings indicate people who are blind are concerned about their physical safety, the security of their information, and the privacy of others. As noted above, findings also indicate people who are blind share pictures they take and are aware of the possibility of unintentionally sharing an embarrassing or sensitive image [3, 42] which may jeopardize their privacy [14]. Our work fills a gap in prior research about privacy concerns for people who are blind, by providing the first study that leads to concrete guidance regarding what content they perceive to be PVC in the context of their VIDS use, and the different conditions that impact their concern for sharing PVC with VIDS.

### 2.4 Taxonomies of Private Visual Content

Several PVC taxonomies have been introduced to support the design of systems that recognize private content in visual media. Most of these taxonomies focus on "how private" an image is (e.g., to be shared only with family, friends, or everyone) [4, 15, 62, 68], while few offer guidance regarding what type of visual content is private [32, 34, 47, 54]. Most related to our work is that of Gurari et al. (2019) [34], who identify 19 types of PVC based on a visual analysis of approximately 40,000 images shared by people who are blind with the VIDS called VizWiz [18]. The authors then developed AI systems to recognize these types of private content in images. In contrast to prior work, in this paper we report our guidelines for a PVC taxonomy created with direct input from people who are blind. We intentionally included in our interviews with people who are blind the PVC types currently supported by systems coming from the AI community to bridge the privacy work between the AI and accessibility communities, so the findings could support immediate, actionable guidance to the AI community.

## 3 STUDY DESIGN

Our study is guided by the following three research questions:

- (1) What factors do people who are blind identify as impacting their privacy in the context of their use of VIDS?
- (2) Which PVC types are of most concern to people who are blind, generally as well as when using H-VIDS versus AI-VIDS?
- (3) How does the intentionality of privacy disclosures affect what they consider to be PVC when using VIDS?

### 3.1 Data Collection

To investigate these research questions, we conducted interviews with 18 participants. Each interview consisted of two parts, which are described below.

**Table 1: Definitions used during the second part of our interviews where we asked study participants to rank their level of concern (top half) with respect to five different conditions (bottom half) for each PVC type.**

Concern Ranking 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 <i>Public</i>
HK		Private Visual Content (PVC) is shared with Human-powered VIDS (H-VIDS) <i>Knowingly</i>
HU		Private Visual Content (PVC) is shared with Human-powered VIDS (H-VIDS) <i>Unknowingly</i>
AK		Private Visual Content (PVC) is shared with AI-powered VIDS (AI-VIDS) <i>Knowingly</i>
AU		Private Visual Content (PVC) is shared with AI-powered VIDS (AI-VIDS) <i>Unknowingly</i>

**3.1.1 Semi-Structured Interview Questions:** The first part of each interview included 21 semi-structured questions about participants' use and preferences for using different VIDS, their understanding of how the services work, the types of visual content they consider to be private, their definitions of "privacy" and "privacy concerns"<sup>2</sup> outside the premise of VIDS. This was important in establishing what privacy concerns naturally emerged and the role VIDS play in the life of each participant prior to introducing them to the pre-established list of PVC. We designed the semi-structured interview section to take approximately 45 minutes.

**3.1.2 Ranking Task:** For the remainder of the interview, we asked participants to rank their level of concern for 21 PVC content types. To establish these PVC types we drew on findings from Gurari et al. [34], who identified 19 types of PVC through a visual analysis of approximately 40,000 images shared by people who are blind. We also added two general PVC types (Name and Location) not defined as unique PVC types in Gurari et al. [34]. We chose to provide the 21 pre-identified PVC content types to participants to ensure that the PVC types we drew on 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.

For each PVC type, we prompted participants with the following question: "Imagine that [the PVC] was shared and became available to the public for anybody to use. How would that make you feel?". In cases when participants expressed a concern, we followed up by asking "Why would it be of particular concern?". These questions enabled us to learn about participants' concerns related to the PVC type agnostic of how the data became available or the type of VIDS they would share their visual information with. After they responded to this prompt and the related questions for one PVC type, we asked participants to rank their level of concern by specifying a score between 1 and 5 (1=Not Concerned/ 5=Extremely

Concerned) in the case that the PVC was publicly shared.<sup>3</sup> We then asked participants to rank their level of concern according to four other conditions, shown in **Table 1**. These four conditions capture how people's privacy concerns change when (1) the agent providing the description was AI-powered versus human-powered and (2) they share their private data knowingly versus inadvertently. For each condition, we also asked participants provide a short explanation of their ranking. In total, each participant was asked to provide 105 responses (i.e., 21 types x 5 conditions). For each participant, we randomized the order of the PVC types.

**3.1.3 Implementation:** We recruited study participants by circulating an IRB-approved announcement on social media, on a list-serv managed by organizations serving people who have visual impairments, and through snowball sampling [58]. 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).

Two researchers conducted the interviews with N=18 participants (11 female/7 male, ages 22-73 years with an average of 42) over the phone in Spring of 2020. One researcher led the interviews while the other took structured notes. All interviews were audio recorded and lasted from 1-2 hours. All participants were located in North America and identified as being totally blind. Ten participants were blind from birth, and eight had acquired blindness. The participants' level of education varied from completion of high school to

<sup>3</sup>When developing this ranking scale we considered using the "Stage of Concern Scale" [37], which has been widely used to rank 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.

<sup>2</sup>Concerns consist of feelings, preoccupations, thoughts, and considerations [37]. In addition, 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 [56, 61].

having received a PhD. When we asked participants which VIDS they used, all participants reported prior use of VIDS that employ humans (e.g., Aira, Be My Eyes) and VIDS that employ AI (e.g., Seeing AI). Ten participants reported using Aira as their primary VIDS, four people specified Be My Eyes as their primary VIDS, and four people specified Seeing AI as their primary VIDS. We assigned a unique identifier for each participant, which is summarized with demographic information in the Supplementary Materials.

## 3.2 Data Analysis

**3.2.1 Semi-Structured Interview Data:** We analyzed the interview data through an integrative process. We began by writing analytic memos after each interview to support our reflection and to identify emergent patterns, categories, and concepts [63]. For the first three interviews, two researchers independently listened to recordings of the interviews independently wrote analytical memos, and then together compared their memos and resolved any disagreements through iterative discussion. For the subsequent 15 interviews, the two researchers took turns 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 [17] as a technique to collaboratively identify and distill themes across the analytic memos. When creating the affinity diagram, we observed that much of the collected data fell into three themes:

- (1) *Understanding of the Service Offering:* Instances when participants reflected on or shared their understanding of how the VIDS deliver their services; this covered both their sense that privacy is at risk and their sense that their privacy is bolstered by VIDS;
- (2) *Personal/ Social Impact:* Instances when participants made statements about the VIDS 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 H-VIDS and AI-VIDS use.<sup>4</sup>

We drew on these themes when conducting an iterative thematic analysis [23] of the interview transcripts. In some cases, we directly coded to segments of the transcripts with codes that were reflective of these themes, and then applied sub-themes to explain the nuance in their responses. In other cases, we first identified the sub-themes, and when applicable categorized them under the primary theme codes. Ultimately, our analysis of the semi-structured interview data resulted in a set of themes and sub-themes which convey the factors that impact how people who are blind perceive privacy in the context of their use of VIDS, including both H-VIDS and AI-VIDS (**RQ1**). In the findings section, we report on these factors according to the three primary themes.

<sup>4</sup>Human values can be understood as "what a person or group of people consider important in life" [31]. 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 [59]. Values are critical for understanding how individuals interact with information [29].

**3.2.2 Ranking Task Data:** After analyzing the semi-structured questions, we analyzed the ranking results by calculating the average scores for each PVC type across the five conditions (**Table 1**) in which the information would be shared. This enabled us to see the participant group's overall level of concern about the disclosure of each type of PVC, according to the five conditions. The resulting data provides the foundation for addressing **RQ2** and **RQ3**.

The data we collected from the ranking task also contained 1890 short-answer responses (21 PVC types x 5 conditions x 18 participants), where participants justified their ranking scores. To observe whether there were common themes within the participants' responses for each PVC (and the five conditions in which that PVC would be shared), we organized the data according to each PVC type and each condition, and assigned a code to each response. After coding three of the PVC types, we observed that some of the emergent codes we were assigning related to the factors we identified during the semi-structured interviews. In turn, we adopted these factors as codes. In other cases, we needed to create new codes to reflect the themes that were emerging from the short-answer ranking responses. For example, in the context of the "Framed Photo" PVC we heard a participant state, "Well, that is probably not very good. That is a good example of why I choose a spot [where I am going to call from] before I use services." For this short-answer response we employed the code *Personal Responsibility to Manage Information*, and organized it under the *Personal/Social Impacts* parent theme (established during the semi-structured interview data analysis). To avoid creating redundant codes across the PVC types, after coding all of the 1890 responses, we sorted and reviewed all the codes and the attached responses in order to merge or reassign revised codes to the applicable responses.

## 4 FINDINGS: PRIVACY RELATED BENEFITS AND RISKS OF VIDS

In this section we present our analysis of the factors that people who are blind identify as adding *benefit* to their sense of privacy and adding *risk* to their sense of privacy in the context of their use of H-VIDS and AI-VIDS (**RQ1**).

### 4.1 Human-powered VIDS: Benefits

**4.1.1 Understanding of the Service Offering.** Several factors related to participants' understanding of how VIDS provide their services. First, we heard a belief or assumption that the H-VIDS 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 H-VIDS *corporate messaging*. For instance, P06 shared she had received emails from Aira which provided her with a sense of trust in the services, though she admitted to not actually reading the policy. (Some participants were aware of VIDS's policies but did not see them as a benefit, which we discuss in the *Risks* section.)

Several participants noted that they perceived H-VIDS to be professional and trustworthy due to internal and public-facing

policies designed to protect users. One policy that participants identified as beneficial to their privacy was the *choice to opt out* or choose not to share their data with the H-VIDS. 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 H-VIDS mandate for agents (sometimes referred to as remote sighted assistants [46]) 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.*” She went on to relate VIDS service offerings with other assistive company policies, “*Aira is track-able, similar to knowing who your Uber driver is.*”

Though related to the professionalism and the internal policies of H-VIDS, we heard participants explicitly note that interacting with *trained agents* is a 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.*”

**4.1.2 Values-Based Assessment.** Some participants explicitly conveyed factors related to their values when describing what they consider to be important when using H-VIDS, and/or and described how the VIDS they use uphold 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 people who are blind knowingly share their PVC. When discussing the benefit of Be My Eyes [28], a volunteer-based H-VIDS, 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. In addition to trust in the remote sighted assistants we heard participants extend their sense of trust 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 H-VIDS like Be My Eyes because these services preserve their *anonymity* when sharing PVC. 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 they encounter when family or friends access their images.

## 4.2 Human-powered VIDS: Risks

**4.2.1 Understanding of the Service Offering.** One prominent theme that we observed is that many participants reported a lack of understanding on VIDS’ 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?*” She 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 [VIDS] try to do that?*”

**4.2.2 Personal/Social Impact.** One of the clearest risks that participants associated with H-VIDS was *identity theft*. We heard concerns that H-VIDS created opportunities for nefarious actors to access their data and illegally use the information for personal gain. For instance, P10 specifically mentioned identity theft as a concern and thus she is “*Not comfortable with another person reading my information.*” Similarly, P18 talked about having trouble setting up an online account, “*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.*”

We heard some participants express a *fear of social judgement* related to their use of H-VIDS, 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 H-VIDS 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.*”

**4.2.3 Values-based Assessment.** Some participants indicated that they were at greater risk when using VIDS 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 H-VIDS, “*I haven’t used the volunteer one because you never know what you’re going to get in terms of quality of the volunteer.*”

## 4.3 AI-powered VIDS: Benefits

**4.3.1 Understanding of the Service Offering.** Most notably, some participants specified that using AI-VIDS 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 [VIDS] stores or can store information, it just moves on.*” Similar to P10, P04 indicated she trusts that AI-VIDS 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-VIDS is that their data is not collected and/or retained by a person (in 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.”

**4.3.2 Personal/Social Impact.** Several study participants indicated that a benefit of AI-VIDS was that they eliminate the risk or sustained *fear of social judgement* (which occurs when using H-VIDS). For instance, P08 stated AI-VIDS 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-VIDS related to privacy is that these services eliminate the possibility of embarrassment or other psychological impact.

**4.3.3 Values-based Assessments.** Similar to H-VIDS, participants indicated that AI-VIDS 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-VIDS offer more anonymity than H-VIDS. P11 stated he valued anonymity provided by AI-VIDS, “for speed efficiency and a little more anonymity.”

## 4.4 AI-powered VIDS: Risks

**4.4.1 Understanding of the Service Offering.** Often, our study participants discussed their lack of understanding of how AI-VIDS handle 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 VIDS policies, raising questions about the length of data retention. Regarding Seeing AI, P05 stated, “I don’t know how long they store information.” It was evident that participants were concerned about how VIDS handle their data, and indicated that the lack of transparency creates a lack of trust. P05 said, “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-VIDS 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, though they were vague about what would make the technology faulty.

## 4.5 Self-identified Private Visual Content

Here we present the types of private visual content that the participants self-identified during the semi-structured portion of the interview. As a reminder, we intentionally solicited these privacy types prior to exposing the participants to predefined PVC types in order to establish what privacy concerns naturally emerged for them.

Some of the PVC types participants shared were similar to the PVC types reported in Gurari et al. [34]. These include: **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, Medicaid, and medical); **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. [34]. Most prominently, eight participants spoke about **Social Security Information**. For instance, P18 explained that people who are blind commonly use their 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 for another person 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 which 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.” Our open-ended questions provided participants an opportunity to consider what they deemed private content, which helped prime them for the ranking exercise that followed.

## 5 FINDINGS: PRIVATE VISUAL CONTENT CONCERNS

In this section, we present an overview of how participants defined the term *privacy concern* generally, as well as their rankings of the level of concerns regarding the 21 PVC types.

### 5.1 Defining Privacy Concern

Prior to presenting participants with the task of ranking the 21 PVC types according to their level of concern, we asked them to define the phrase “privacy concern” in their own words.

In response, several participants focused on privacy being a safeguard. For instance, 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. P07 said, “Privacy means personal control over information that was not necessarily intended for a wide distributed audience.” Participants also discussed privacy in terms of personal management. For example, 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.”

As exemplified above, some participants defined privacy concerns in terms of what is NOT being safeguarded or the loss of control, ownership, or the ability to manage. 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 the malicious acts of others including P17 who identified “A breach of my personal information...[use by] someone who will go to the effort to delete their tracks.”

Finally, throughout the interviews we heard participants directly identify 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 upfront, but it’s hard to know what is out there. My identity is on the line and I need protection too.”

## 5.2 Private Visual Content Clusters

Here we present the ranking results in Table 2. The ranking findings serve as the foundation to address **RQ2** and **RQ3**. We discuss below the major trends that we observe. In particular, we provide in-depth descriptions of the participants’ reasons for concern for the PVC of the most concern (financial account information) and provide a more general overview for the other PVC concerns.

**5.2.1 Financial Information.** Reinforcing the participants’ self-reported findings, the ranking findings show people who are blind consider financial account information to be the most concerning PVC. Here we present this finding according to the five different conditions (Table 1):

**Public.** The average ranking was 4.6 out of 5 (**Table 2, Row 1**), with 16 participants ranking public availability of their financial information as extremely concerning, based on the concerns 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, a sense of *loss of control or agency*, or *social judgement*. In one instance, a participant indicated that financial information is an *intimate personal experience*.

**H-VIDS.** Participants’ concerns were dramatically lower when sharing this PVC *knowingly* with H-VIDS; i.e., a drop from 4.6 in the public context to 2.8. Those who did express concern or extreme concern specified *financial theft*, *unwanted identity disclosure*, and *unknown data retention or disclosure policies* as reasons. We attribute the majority of the responses which indicated lower concern to participants’ *need for the information* or their understanding of the *professionalism* of the VIDS, that their data would be *protected*

*by policy*. That said, the participants’ concerns were higher (3.5) in the situation that their financial account information would be shared *unknowingly* with a H-VIDS. The primary reasons for this 0.4 point increase can be attributed to the participants’ *fear of lack of personal management*, that the sharing of this information was *outside their realm of personal awareness-control*, *loss of control or agency*, in addition to many of the aforementioned concerns.

**AI-VIDS.** Participants concerns when *knowingly* sharing PVC with AI-VIDS dropped lower than observed for *knowingly* sharing PVC with H-VIDS *Knowingly*; i.e., a drop of 0.3 to 2.5. Only two participants expressed extreme concern in this situation, based on fear of *financial theft* or *unwanted identity disclosure*. Other concerns included: *unknown data retention or disclosure policies* and the *need to protect others*. Those who expressed less concern reasoned that they *needed the 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 the data* or that the *data is only on the device*. 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 AI-VIDS, the average score increased to a 3.1. This trend is similar to what we observed with H-VIDS. This increase can be attributed to the participants’ *fear of lack of personal management* and the *unknown data retention or disclosure policy* in addition to many of the aforementioned concerns.

**5.2.2 Medical Information.** We observed almost as high of a level of concern from participants regarding medical information as observed for financial information (**Table 2, IDs 2-4**), though for different reasons. For example, the participants who expressed extreme concern that any of their medical information (ID: 2) would be publicly shared, offer the following reasons: it *reveals intimate personal experience*, *undefined threat/consequence*, *social judgement*, *against HIPPA*, *need to protect others*, and *content dependent*. Participants concerns were lower when thinking about sharing medical information with H-VIDS or AI-VIDS than publicly; e.g., 4.2 for sharing publicly versus 2.9 and 3.4 for sharing with H-VIDS *knowingly* and *unknowingly* respectively (**Table 2, ID 2**). Participants’ considerations for sharing with H-VIDS included: *professionalism* of the service, being *protected by policy*, a *trust of human decency*, or simply because they *needed information*. Participants’ considerations for sharing with AI-VIDS *knowingly* included: *data only on device*, *no human eyes on data*, or *personal data is anonymized* (though there were still plenty of reasons that they were concerned). Similar to what we observed for the financial information, we found the prospect of *unknowingly* sharing medical PVC with either H-VIDS or AI-VIDS was slightly higher than when *knowingly* sharing the same information.

**5.2.3 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 (**Table 2, IDs 5-8**), images showing a *naked body* was of greatest concern—with only slight variation in the participants’ concerns across the conditions that it would be shared Publicly (4.1) or with H-VIDS, *Knowingly* (4.0) or *Unknowingly* (4.1). The concerns participants expressed regarding the disclosure of an image of a naked body included: *damage to [their] reputation*, *social judgement*, *disclosure of their identity*, or would be *grounds for termination of use* of the VIDS. In addition, they expressed the

**Table 2: Results from the ranking data analysis. PU=Private Visual Content (PVC) is shared with the *Public*; HK=Private Visual Content (PVC) is shared with Human-powered VIDS (H-VIDS) *Knowingly*; HU=Private Visual Content (PVC) is shared with Human-powered VIDS (H-VIDS) *Unknowingly*; AK=Private Visual Content (PVC) is shared with AI-powered VIDS (AI-VIDS) *Knowingly*; AU=Private Visual Content (PVC) is shared with AI-powered VIDS (AI-VIDS) *Unknowingly*.\*=Replicated PVC Type. [\*] Indicates repeated PVC type because it falls under two clusters.**

ID	PVC Types	Conditions				
		PU	HK	HU	AK	AU
<b>Financial</b>						
1	Account Information	4.6	2.8	3.4	2.5	3.1
<b>Medical</b>						
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
<b>People</b>						
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
<b>Location</b>						
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	Location	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
<b>Identification</b>						
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
<b>Computer/Online Access</b>						
20	Computer Screen w. Username	2.8	1.5	1.9	1.6	2.0
<b>Affiliation</b>						
21	Clothing with a Logo	1.3	1.3	1.4	1.1	1.3
<b>Average Score</b>		<b>2.8</b>	<b>1.8</b>	<b>2.1</b>	<b>1.8</b>	<b>1.8</b>

*fear of lack of personal management*, the *need to protect others*, 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-VIDS, *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.

**5.2.4 Identification and Location Information.** We focused for this cluster on the PVC types which revealed one's *location* (rather than those that would reveal one's *name*). We observe greater concern,

as manifested through higher scores, when the content is more personal (**Table 2, IDs 9-19**). For instance, participants showed low concern for newspapers with the name of the city shown or the name of a local library branch (which were identified as *public information*), whereas letters, personal names, or one's address were of more concern.

**5.2.5 Location.** This sub-cluster included 8 PVC types (**Table 2, IDs 9-16**). The ranking findings show that paperwork showing a name and/or an address publicly were of highest concern for participants (**Table 2, IDs 9-10**). The findings also show participants understood an address would be more concerning than location information because an address could locate their home whereas a general location could only indicate their position at a single point in time. As with other PVC clusters, across all of these PVC types,

we observed participants were more concerned in situations where the PVC was shared with AI-VIDS *unknowingly*.

**5.2.6 Name.** As above, in this sub-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 number (**Table 2, ID 20**) ranking fell between mildly concerning and concerning, some participants ranked this PVC type as very or extremely concerning because they understood license plate information to be a risk *if paired with other information/metadata* and that it represented an *unwanted identity disclosure* or an *undefined threat/consequence*. We also commonly heard participants explain that by sharing license plate information they could be violating others' privacy and their *need to protect others*.

**5.2.7 Computer/Online Access.** We heard participants concerns about a username (**Table 2, ID 20**) being shown, particularly in the case that it was shared publicly or *unknowingly* with VIDS. Participants were concerned sharing this PVC 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 realm of personal awareness-control*. We also heard a particular concern of the threat that malicious actors could pose if this PVC was *paired with other information*.

**5.2.8 Affiliation.** One PVC type fit under this cluster: a piece of clothing with a logo (**Table 2, ID 21**). In the few instances participants gave a higher ranking to this PVC, the concern centered on *damage to [their] reputation*, or *social judgement*. Under the condition of sharing this PVC type *unknowingly* with H-VIDS or AI-VIDS, participants worried the sharing would be *outside [their] realm of personal awareness-control* or cause *fear [related to their] lack of personal management*.

## 6 DISCUSSION

### 6.1 User-Centered PVC Taxonomy

Our findings in **Table 2** provide the first discussion about a PVC taxonomy originating from people who are blind. We offer this as a valuable foundation for training VIDS employees and volunteers as well as developers of automated VIDS to incorporate stricter data handling features and protocols. In its current form, we expect the taxonomy to guide concrete, actionable next steps for improving upon the status quo of H-VIDS and AI-VIDS to reflect their users' privacy concerns. This taxonomy also can provide actionable guidance for policy makers in deciding which types of PVC, if any, can be stored, sold, and used. Furthermore, our findings may offer an important user-driven foundation for grounding future regulation in real users' interests, including for EU's General Data Protection Regulation (GDPR).

### 6.2 The Impact of PVC Disclosures

While the PVC taxonomy provides a useful snapshot of our participants' levels of concerns about each PVC in the context of their VIDS use, our reporting of the factors that impact their sense of privacy adds insight into the complexity of privacy in the context of VIDS use. The *risks* and *benefits* factors that we identified show

that privacy in the context of VIDS use is complex, and should also be examined according to (A) the specific type of VIDS offering the interpretation, and (B) the specific characteristics of each PVC type. Regarding how selection of H-VIDS versus AI-VIDS affects privacy, we observed that one type of service may offset the concerns raised by another. For example, under the condition that a pregnancy test result is shared with a H-VIDS (*knowingly* or *unknowingly*), we learned that some participants fear other peoples' judgement. Conversely, we heard that the fear of judgement is eliminated when such a PVC is shared with an AI-VIDS (*knowingly* or *unknowingly*), reinforcing findings from previous work [11].

More generally, our analysis reveals a novel finding that each PVC solicits unique sets of concerns, and that the level of concern changes according to the condition in which it is shared (*knowingly/unknowingly* and H-VIDS/AI-VIDS). For example, the *risks* associated with disclosure of information on a *pill bottle* differed from what makes disclosure of a *letter with a name and/or address* concerning, despite the fact that they have the same concern scores across four conditions. In turn, we recommend that when drawing on the PVC taxonomy as a guide, VIDS developers remember that the concerns connected to one PVC may be entirely different from another type of PVC and may shift as depending on who and if they are using humans or AI to provide the interpretations. These differences may require VIDS agents to handle the collection, storage, and retention of each PVC type differently.

### 6.3 Understanding of Data Handling and VIDS

In addition to the factors adding *benefit* or *risk* to VIDS, our findings show the ways VIDS communicate about their collection, retention, or selling of visual data is not assessable [30] or well-understood by people who are blind. Within the semi-structured interview findings we reported this as *unknown data handling*, a *risk* affecting both H-VIDS and AI-VIDS. Even when participants demonstrated that they had understanding or positive impressions of how VIDS handle their data (*professionalism*, *trained agents*, and the *choice to opt*), they commonly raised questions about the way their data is handled. The ranking data findings affirmed that VIDS visual data handling policies are of concern to participants; we applied the *unknown data handling* code 117 times<sup>5</sup>.

More generally, throughout the interviews we observed variance in the ways participants understood how VIDS technically work. Though many participants understood that H-VIDS use trained agents or volunteers, they had little understanding of how these agents were selected. Their understanding of how AI-VIDS work varied greatly; some participants explained AI-VIDS still depend on human-agents to describe the content, whereas others perceived it as a black box, and still others described in technical detail how AI-VIDS use machine learning. We also observed that whereas some participants had very specific notions of privacy in relation to VIDS, others shared they had not thought of it before. In fact, many participants indicated these interviews provided them a unique opportunity to think about privacy in the context of their VIDS use. These findings indicate efforts are needed to ensure VIDS terms of

<sup>5</sup>12 times across 11 PVC types for PVC shared with H-VIDS *knowingly*; 14 times across 10 PVC types for PVC shared with H-VIDS *unknowingly*; 35 times across 17 PVC types for PVC shared with AI-VIDS *knowingly*; and 55 times across 18 PVC types for PVC shared with AI-VIDS *unknowingly*.

service, privacy polices, and underlying technologies are assessable [30] and comprehensible by users.

#### 6.4 Privacy Values and Trade-Offs

Friedman et al. (2008) [31] identify and define privacy as a core value implicated in systems design, and define it as “*a claim, an entitlement, or a right of an individual to determine what information about himself or herself can be communicated to others.*” Our investigation into the factors that impact our participants’ senses of privacy in the context of their VIDS use revealed eight values closely aligned with privacy. In particular, we observed that participants directly articulated three key values during the semi-structured interviews. Those that were explicitly referenced include: *[trust in] human decency, anonymity, and accountability*. During the ranking activity the participants also made statements directly related to their: *control/ownership, consent, acceptability, care/protection of others, and rights/justice*.

The other factors that emerged during the interviews can also be related to underlying values, though we were cautious not to ascribe these values to the participants’ responses without explicit reference. For example, the codes *wouldn’t share intentionally* and *unwanted identity disclosure* may be related to the value of control and ownership, where as the codes *identity theft, financial theft, and locate person* can relate to the value of *consent*. Other codes can be attributed to the values of acceptability/freedom from bias including *social judgement, damage to reputation, and not socially acceptable*.

Though Friedman et al. (2008) similarly identify human welfare, ownership and property, trust, courtesy, autonomy, informed consent, and accountability as values in their Value-Sensitive Design frameworks, and while other work has looked at privacy related to disability status in the context of social media use [51], to our knowledge no prior work has looked at privacy in the context of VIDS, nor identified the privacy-adjacent values in the context of VIDS development. The values we identified can be used to examine which VIDS are in alignment with their users’. Furthermore, they may be used to design features and/or terms of service to ensure services are not exploitative of their users’ data.

#### 6.5 PVC Protections for People Who Are Blind and Beyond

We designed this study to focus on privacy in the context of blind users’ experiences with VIDS based on our understanding that this population is at particular risk for sharing images that contain PVC [34]. In fact, during the interviews we heard participants directly identify that their blindness increases their need for privacy protections, which is in alignment with previous work [38].

To our knowledge, this is one of the first efforts to ensure representation of people who are blind at a time when VIDS are quickly changing their service offerings and management strategies (e.g., Aira was sold to another owner at the end of our interviews), and computer vision developers are investigating how to use AI to expand their service offerings. Further, our work responds to contemporary calls to “*protect people who fall outside of the ‘norms’ reflected and constructed by AI systems*” [40] and to develop AI systems based in ethical considerations [50, 66].

Our findings also revealed factors beyond visual impairment that impact how a person conceives of privacy in the context of their VIDS use (e.g., prior visual experience, education, socioeconomic status), reinforcing the importance of intersectionality. We hypothesize our findings about people’s need for privacy in the context of the images they take and share transcend the blind population. In an era when unregulated collection, storage, and selling of visual data is abundant, everyone may face loss of control of PVC, the nefarious use of such information, or confusion around terms of service. We expect the contributions we make in this paper to generalize to other services that handle visual data that is *knowingly* or *unknowingly* shared by their users.

#### 6.6 Limitations and Future Work

Importantly, several limitations of this study should be held in consideration when using our findings. First, during the ranking task, participants wanted more context for some of the PVC types to provide a confident answer. For instance, under the *information designation* child code, we identified 111 instances where participants stated their answer would change based on the specifics of the image content, including 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.

Second, the values we identified during our analysis brought to light that participants often must compromise one value for another in the context of their VIDS use. Early findings show that three types of trade-offs, occur in this context: (1) A person’s willingness to compromise their value of personal privacy for *access, independence, convenience, interactivity, or public service*; (2) The circumstances in which participants must forgo the values that constitute privacy, for instance one may need to relinquish ownership, diminishing the power of their consent over how their PVC is handled to get the information they need; and (3) The circumstances in which participants forgo use of one type of VIDS and use another because it does not align with their values. We aim to explore these trade-offs in future work.

We believe there are numerous additional user studies that would be valuable to conduct. This includes contextual inquiries to better understand the lived practices and behaviors that people who are blind enact at the micro or macro level to preserve their PVC, and how the experiences and values of remote visual assistants align with users. In addition, we plan to conduct focus groups with people who are blind to rewrite privacy policies that reflect their values. Another valuable direction for future work is to elucidate users’ privacy preferences with VIDS for factors such as camera form factor as well as with respect to hybrid VIDS that leverage both AI and humans. Finally, it would be interesting to examine whether the *benefits and risks* we identified regarding PVC generalize beyond people who are blind.

## 7 CONCLUSION

We conducted an empirical investigation into the types of visual content people who are blind consider to be private in the context of their use of VIDS. We identified factors that benefit one's sense of privacy and factors that add risk to one's sense of privacy. Some of these factors describe actual or perceived impact on one's sense of personal or societal well-being. Towards improving VIDS, such that they provide users with stronger privacy protections and a sense of control of their information, we identified what types of visual content are most concerning to people who are blind. More generally, we offer our findings as a guide to implement stricter protocol around how private visual data is handled and employ values to ensure that VIDS are developed in alignment with their users.

## ACKNOWLEDGMENTS

We would like to thank Jaxsen Day for helping pilot our interview protocol. This work was supported by Good Systems, a research grand challenge at the University of Texas at Austin.

## REFERENCES

- [1] Ali Abdolrahmani, Ravi Kuber, and Stacy M Branham. 2018. Siri Talks at You: An Empirical Investigation of Voice-Activated Personal Assistant (VAPA) Usage by Individuals Who Are Blind. In *Proceedings of the 20th International ACM SIGACCESS Conference on Computers and Accessibility*. ACM, 249–258.
- [2] AbleData. 2020. Color Teller Talking Color Identifier. <https://abledata.acl.gov/product/color-teller-talking-color-identifier>. (Accessed on 01/08/2020).
- [3] Dustin Adams and Sri Kurniawan. 2014. A blind-friendly photography application for smartphones. *ACM SIGACCESS Accessibility and Computing* 108 (2014), 12–15.
- [4] 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.
- [5] Tousif Ahmed. 2019. *Towards the Design of Wearable Assistive Technologies to Address the Privacy and Security Concerns of People with Visual Impairments*. Ph.D. Dissertation. Indiana University.
- [6] 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*. ACM, 3523–3532.
- [7] 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.
- [8] Seeing AI. 2020. Talking camera app for those with a visual impairment. <https://www.microsoft.com/en-us/ai/seeing-ai>. (Accessed on 01/08/2020).
- [9] Alpoly. 2020. Alpoly Homepage. <https://www.alpoly.com/>. (Accessed on 01/08/2020).
- [10] Aira. 2020. Aira Homepage. <https://aira.io/>. (Accessed on 01/08/2020).
- [11] 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)*. USENIX Association, Boston, MA. <https://www.usenix.org/conference/usenixsecurity20/presentation/akter>
- [12] Shiri Azenkot, Sanjana Prasain, Alan Borning, Emily Fortuna, Richard E Ladner, and Jacob O Wobbrock. 2011. Enhancing independence and safety for blind and deaf-blind public transit riders. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*. ACM, 3247–3256.
- [13] Shiri Azenkot, Kyle Rector, Richard Ladner, and Jacob Wobbrock. 2012. Pass-Chords: Secure Multi-touch Authentication for Blind People. In *Proceedings of the 14th International ACM SIGACCESS Conference on Computers and Accessibility (Boulder, Colorado, USA) (ASSETS '12)*. ACM, New York, NY, USA, 159–166. <https://doi.org/10.1145/2384916.2384945>
- [14] Cynthia L Bennett, Martez E Mott, Edward Cutrell, Meredith Ringel Morris, et al. 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, 76.
- [15] 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.
- [16] BeSpecular. 2020. BeSpecular. <https://www.bespecular.com/>. (Accessed on 01/08/2020).
- [17] Hugh Beyer and Karen Holtzblatt. 1998. Contextual design: defining customer-centered systems. 1998. *San Francisco: Morgan Kaufman* (1998).
- [18] Jeffrey P Bigham, Chandrika Jayant, Hanjie Ji, Greg Little, Andrew Miller, Robert C Miller, Robin Miller, Aubrey Tatarowicz, Brandyn White, Samuel White, et al. 2010. VizWiz: nearly real-time answers to visual questions. In *Proceedings of the 23rd annual ACM symposium on User interface software and technology*. ACM, 333–342.
- [19] 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*. ACM, 3–10.
- [20] Erin Brady, Meredith Ringel Morris, and Jeffrey P Bigham. 2015. Gauging receptiveness to social microvolunteering. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 1055–1064.
- [21] 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 (Paris, France) (CHI '13)*. ACM, New York, NY, USA, 2117–2126.
- [22] 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, 260–269.
- [23] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.
- [24] Daniella Briotto Faustino and Audrey Girouard. 2018. Understanding authentication method use on mobile devices by people with vision impairment. In *Proceedings of the 20th International ACM SIGACCESS Conference on Computers and Accessibility*. ACM, 217–228.
- [25] Shonal Chaudhry and Rohitash Chandra. 2015. Design of a mobile face recognition system for visually impaired persons. *arXiv preprint arXiv:1502.00756* (2015).
- [26] Tai-Yin Chiu, Yinan Zhao, and Danna Gurari. 2020. Assessing Image Quality Issues for Real-World Problems. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 3646–3656.
- [27] Bryan Dosono, Jordan Hayes, and Yang Wang. 2015. "I'm Stuck!": A Contextual Inquiry of People with Visual Impairments in Authentication. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 151–168. <https://www.usenix.org/conference/soups2015/proceedings/presentation/dosono>
- [28] Be My Eyes. 2020. Bringing sight to blind and low-vision people. <https://www.bemyeyes.com/>. (Accessed on 01/08/2020).
- [29] Kenneth R Fleischmann. 2013. Information and human values. *Synthesis Lectures on Information Concepts, Retrieval, and Services* 5, 5 (2013), 1–99.
- [30] Andrea Forte, Nazamin Andalibi, Thomas Park, and Heather Willever-Farr. 2014. Designing information savvy societies: an introduction to assessability. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2471–2480.
- [31] 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.
- [32] Andrea Frome, German Cheung, Ahmad Abdulkader, Marco Zenarro, 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.
- [33] 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*. 3511–3522.
- [34] 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.
- [35] 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.
- [36] Danna Gurari, Yinan Zhao, Meng Zhang, and Nilavra Bhattacharya. 2020. Captioning Images Taken by People Who Are Blind. *arXiv preprint arXiv:2002.08565* (2020).
- [37] Gene E Hall et al. 1977. Measuring Stages of Concern about the Innovation: A Manual for the Use of the SoC Questionnaire. (1977).
- [38] 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*.
- [39] iDentifi. 2020. iDentifi. <http://getidentifi.com/>. (Accessed on 01/08/2020).

- [40] AI Now Institute. 2019. Disability, Bias, and AI. <https://ainowinstitute.org/disabilitybiasai-2019.pdf>. (Accessed on 01/02/2020).
- [41] 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.
- [42] 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*. ACM, 203–210.
- [43] 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 *Proceedings of the 11th International ACM SIGACCESS Conference on Computers and Accessibility* (Pittsburgh, Pennsylvania, USA) (*Assets '09*). ACM, New York, NY, USA, 115–122. <https://doi.org/10.1145/1639642.1639663>
- [44] KM Kramer, DS Hedin, and DJ 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.
- [45] Kyungjun Lee, Daisuke Sato, Saki Asakawa, Hernisa Kacorri, and Chieko Asakawa. 2020. 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* (Honolulu, HI, USA) (*CHI '20*). Association for Computing Machinery, New York, NY, USA, 1–12. <https://doi.org/10.1145/3313831.3376398>
- [46] Sooyeon Lee, Madison Reddie, Chun-Hua Tsai, Jordan Beck, Mary Beth Rosson, and John M Carroll. 2020. 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*. 1–12.
- [47] 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* (Honolulu, HI, USA) (*CHI '20*). Association for Computing Machinery, New York, NY, USA, 1–14. <https://doi.org/10.1145/3313831.3376498>
- [48] Sylvan Lobo, Ulemba Hirom, VS Shyama, Mridul Basumatori, and Pankaj Doke. 2017. Coping with Accessibility Challenges for Security-A User Study with Blind Smartphone Users. In *IFIP Conference on Human-Computer Interaction*. Springer, 3–22.
- [49] LookTel. 2020. Instant Recognition Apps for Persons with Low Vision or Blindness. <http://www.looktel.com/>. (Accessed on 01/08/2020).
- [50] Meredith Ringel Morris. 2019. AI and Accessibility: A Discussion of Ethical Considerations. *arXiv preprint arXiv:1908.08939* (2019).
- [51] Meredith Ringel Morris, Annuska Zolyomi, Catherine Yao, Sina Bahram, Jeffrey P Bigham, and Shaun K Kane. 2016. "With most of it being pictures now, I rarely use it" Understanding Twitter's Evolving Accessibility to Blind Users. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. 5506–5516.
- [52] Maia Naftali and Leah Findlater. 2014. Accessibility in context: understanding the truly mobile experience of smartphone users with motor impairments. In *Proceedings of the 16th international ACM SIGACCESS conference on Computers & accessibility*. ACM, 209–216.
- [53] OrCam. 2020. Never Forget a Face. <https://myme.orcam.com/>. (Accessed on 04/21/2020).
- [54] Tribhuvanesh Orekondy, Bernt Schiele, and Mario Fritz. 2017. Towards a visual privacy advisor: Understanding and predicting privacy risks in images. In *Proceedings of the IEEE International Conference on Computer Vision*. 3686–3695.
- [55] Color Blind Pal. 2020. Color Blind Pal. <https://colorblindpal.com/>. (Accessed on 01/08/2020).
- [56] Sören Preibusch. 2013. Guide to measuring privacy concern: Review of survey and observational instruments. *International Journal of Human-Computer Studies* 71, 12 (2013), 1133–1143.
- [57] KNFB Reader. 2020. App features the best OCR. Turn print into speech or Braille instantly. iOS 3 now available. | KNFB Reader. <https://knfbreader.com/>. (Accessed on 01/08/2020).
- [58] Georgia Robins Sadler, Hau-Chen Lee, Rod Seung-Hwan Lim, and Judith Fullerton. 2010. Recruitment of hard-to-reach population subgroups via adaptations of the snowball sampling strategy. *Nursing & health sciences* 12, 3 (2010), 369–374.
- [59] 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.
- [60] Kristen Shinohara and Jacob O Wobbrock. 2011. In the shadow of misperception: assistive technology use and social interactions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 705–714.
- [61] H Jeff Smith, Sandra J Milberg, and Sandra J Burke. 1996. Information privacy: measuring individuals' concerns about organizational practices. *MIS quarterly* (1996), 167–196.
- [62] 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* (Santiago, Chile) (*HT '14*). ACM, New York, NY, USA, 136–147. <https://doi.org/10.1145/2631775.2631803>
- [63] Anselm L Strauss. 1987. *Qualitative analysis for social scientists*. Cambridge university press.
- [64] TapTapSee. 2020. Blind and Visually Impaired Assistive Technology - powered by CloudSight.ai Image Recognition API. <https://taptapseeapp.com/>. (Accessed on 01/08/2020).
- [65] ToolWiz. 2020. Homepage. [http://www.toolwiz.com/lead/toolwiz\\_eye/](http://www.toolwiz.com/lead/toolwiz_eye/). (Accessed on 04/21/2020).
- [66] Yang Wang. 2017. The Third Wave?: Inclusive Privacy and Security. In *Proceedings of the 2017 New Security Paradigms Workshop* (Santa Cruz, CA, USA) (*NSPW 2017*). ACM, New York, NY, USA, 122–130. <https://doi.org/10.1145/3171533.3171538>
- [67] Hanlu Ye, Meethu Malu, Uran Oh, and Leah Findlater. 2014. Current and future mobile and wearable device use by people with visual impairments. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 3123–3132.
- [68] Sergej Zerr, Stefan Siersdorfer, Jonathon Hare, and Elena Demidova. 2012. Privacy-aware image classification and search. In *Proceedings of the 35th international ACM SIGIR conference on Research and development in information retrieval*. ACM, 35–44.
- [69] 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*. ACM, 2353–2362.