Understanding Emerging Obfuscation Technologies in Visual Description Services for Blind and Low Vision People

RAHAF ALHARBI, University of Michigan, USA
ROBIN N. BREWER, University of Michigan, USA
SARITA SCHOENEBECK, University of Michigan, USA

Blind and low vision people use visual description services (VDS) to gain visual interpretation and build access in a world that privileges sight. Despite their many benefits, VDS have many harmful privacy and security implications. As a result, researchers are suggesting, exploring, and building obfuscation systems that detect and obscure private or sensitive materials. However, as obfuscation depends largely on sight to interpret outcomes, it is unknown whether Blind and low vision people would find such approaches useful. Our work aims to center the perspectives and opinions of Blind and low vision people on the potential of obfuscation to address privacy concerns in VDS. By reporting on interviews with 20 Blind and low vision people who use VDS, our findings reveal that popular research trends in obfuscation fail to capture the needs of Blind and low vision people. While obfuscation might be helpful in gaining more control, tensions around obfuscation misrecognition and confirmation are prominent. We turn to the framework of interdependence to unpack and understand obfuscation in VDS, enabling us to complicate privacy concerns, uncover the labor of Blind and low vision people, and emphasize the importance of safeguards. We provide design directions to move the trajectory of obfuscation research forward.

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

Additional Key Words and Phrases: Blind and Low Vision, Visual Description Services, Privacy, Obfuscation, Qualitative, Speculative and Future Technology, Interdependence

ACM Reference Format:
Rahaf Alharbi, Robin N. Brewer, and Sarita Schoenebeck. 2022. Understanding Emerging Obfuscation Technologies in Visual Description Services for Blind and Low Vision People. *Proc. ACM Hum.-Comput. Interact.* 6, CSCW2, Article 469 (November 2022), 33 pages. https://doi.org/10.1145/3555570

1 INTRODUCTION

Blind and low vision people use visual description services (VDS[1]) to build access in a world that privileges sight and visual sense-making. By enabling their phone cameras, Blind and low vision people use VDS for a variety of everyday experiences such as preparing a meal, picking an outfit, and watching the sunset [12, 31, 50, 121]. Broadly, VDS are divided into three categories based on the modality that conducts the description process: artificial intelligence (AI)-powered (e.g., Seeing

[1]A note on language: in this paper, VDS refers to Visual Description Services. This is not to be confused with Value Sensitive Design (VSD) [59]. Additionally, we recognize individual preferences in disability communities between identity first and person first language [69]. Throughout this paper, we use identity first descriptions.

Authors' addresses: Rahaf Alharbi, rmalharb@umich.edu, University of Michigan, USA; Robin N. Brewer, rnbrew@umich.edu, University of Michigan, USA; Sarita Schoenebeck, yardi@umich.edu, University of Michigan, USA.

2573-0142/2022/11-ART469 $15.00
https://doi.org/10.1145/3555570

AI[2]), human-powered (e.g., Be My Eyes[3] and Aira[4]), and a combination of AI and human-powered (e.g., VizWiz) [31]. Despite their many benefits, VDS have harmful implications. Like any camera based system, VDS have significant privacy and security concerns that lead to potential harms such as identity theft [8, 12, 116].

In response to such tensions, researchers are beginning to develop technical solutions to mitigate privacy concerns and to enable a greater sense of security when using VDS. Primarily, past work suggests and develops computer vision based obfuscation (hereinafter referred to as obfuscation) to alter visual content (e.g., images and videos) by applying image filters (e.g., blur or mask) as way to limit information sharing [15, 66, 90]. Although focused on sighted people, HCI researchers found that obfuscation increases comfort because participants could *see* that obfuscation addresses privacy concerns [15, 39]. Accessibility scholars identified privacy concerns in VDS [12, 66, 116], and suggested and introduced obfuscation algorithms that detect and filter such content [12, 66]. Obfuscation is thought and assumed to be a future direction that addresses privacy concerns within VDS. However, the perspectives of Blind and low vision people on obfuscation are missing. It is unknown if Blind and low vision people would find obfuscation useful in responding to privacy concerns and to what extent.

To fill this gap, we aim to understand and design obfuscation systems *for* and *with* Blind and low vision people. We take inspiration from past HCI and CSCW work that advocates for including stakeholders early in the development of emerging technologies [22, 79, 109, 127, 131]. In particular, we recognize that disengaged technology interventions are contested in the disability community [114, 119, 127–129]. There is a disconnect between the aims of technology and the desires of disabled people [114]. For example, Brewer and Kameswaran found that common design trends in autonomous vehicles fail to capture the needs of Blind people [44]. Disability studies scholar, Ashley Shew, coined the term "technoableism" to account for the increased hype of emerging technologies that claim to celebrate values such as empowerment and independence while upholding harmful, ableist, tropes [114]. Bennett et al. call upon HCI researchers to seriously consider the challenges of adding AI into assistive technologies by attending to care work [28] and interdependence [23]. Because there is often misalignment between emerging technologies and disability communities, this work centers the expertise of Blind and low vision people early in the process rather than after technology has been widely distributed. We explore the broad research question: how do Blind and low vision people want to experience and engage with obfuscation?

We report findings from 20 interviews with Blind and low vision people who use VDS. We found that popular approaches for obfuscation may not align with the needs of Blind and low vision people. Participants refused many aspects of automatic obfuscation approaches. Instead, they wanted to be actively involved in the obfuscation process by choosing and determining obfuscation decisions. Our analysis also described obfuscation use cases, opportunities and challenges. Further, we detailed tensions with (non)visually confirming and interpreting obfuscation outcomes, suggesting solutions to establish trust.

This study has three main contributions. First, our analysis provides an empirical understanding of the perspectives and opinions of Blind and low vision people on privacy and obfuscation. Second, we situate our findings within the framework of interdependence [23, 68, 84] to further unpack and understand the needs and tensions of Blind and low vision people in obfuscation technologies. In thinking through interdependence, obfuscation, and VDS, we complicate the current understanding of privacy needs as it relates to access and identity, we uncover and pay attention to the labor Blind

[2]Seeing AI: www.microsoft.com/en-us/seeing-ai
[3]Be My Eyes: https://www.bemyeyes
[4]Aira: https://aira.io/

and low vision people *already* perform with VDS, and we emphasize the importance of safeguards when errors occur. Third, we offer design directions to improve future obfuscation technologies in VDS.

2 RELATED WORK

In this section, we review work on visual description services (VDS) and disability studies-inspired frameworks to design such systems. We then describe potential concerns of VDS, particularly as they relate to error and privacy concerns. Lastly, we describe obfuscation and its potential for preserving privacy in visual contexts.

2.1 Visual Description Services (VDS)

Over the past decade, numerous types of access technologies emerged to provide Blind and low vision people access with visual information about texts, objects or scenery. For example, social media sites such as Facebook and Instagram began enabling automatic alternative text (alt text) for images [133]. Another type of technology, broadly framed as visual description services (VDS), surfaced to help Blind and low vision people alleviate everyday accessibility barriers. Blind and low vision people use VDS to watch the sunset, knit, cook, archive memories and many other activities [21, 36, 50].

VDS can be categorized based on accepted input and type of visual recognition agent. Some AI-powered services (e.g., Seeing AI) take images as input to provide descriptive information about everyday objects, texts, and faces [12, 40, 116], whereas other human-generated and combination services may take a live-feed video or images as inputs (e.g., Aira and Be My Eyes). Human-generated services can also be categorized based on the type of description providers. Typically, they may be volunteers, friends, crowdworkers, or professionally trained agents [12, 35]. With this diversity in types of VDS, one type might be more successful than others in specific tasks.

The nature of how Blind and low vision people use VDS depends on the type of VDS. Generally, AI-generated VDS are thought to complete tasks such as reading text and barcodes [99]. Some AI-generated VDS offer facial recognition capabilities (e.g. identifying age, gender, hair color and emotional expressions) [4]. Branham et al. suggest opportunities for VDS services to use facial recognition technologies to help Blind people negotiate personal safety considerations [40]. Human-generated VDS are often used for complex tasks. For example, Aira, a VDS that uses trained agents and has affordances in place to support confidentiality, is often used to get descriptions for financial related documents [2, 12, 116], recognize the details of a vehicle in ride-sharing services [45], and help in outdoor navigation [2]. The VizWiz project [31] used crowdworkers to answer visual questions requested by Blind people in seconds, including subjective questions around fashion and color matching that are outside the capacity of AI-enabled VDS [50]. To investigate the use of varying description providers (e.g., volunteers or friends), Akter et al. report that people with visual impairments care about maintaining good impressions with friends than family, thus they might feel more comfortable with crowd workers due to weaker ties and expectations [12].

To address the specific visual needs of Blind people and build appropriate VDS, HCI and accessibility scholarship have begun taking a 'disability-centric approach' [120]. There have been many calls to actively include disabled people as experts and designers of AI and assistive technologies (including VDS systems) [30, 98, 100, 122]. In response, a number of research projects emerged. For example, the IncluSet enables accessibility researchers and community members to locate and contribute public datasets in hopes of improving the performance of machine learning technologies [82]. Through the ORBIT project [5], Theodorou et al. aim to develop systems and algorithms that

[5]More information on the ORBIT project: https://orbit.city.ac.uk/

respond to the unique needs and uses of Blind people by engaging the community in the data collection process [120]. In this paper, we continue building from past work that center the perspectives of disabled people, specifically Blind people, in designing and imaging potential future additions (obfuscation) to VDS.

2.2 Interdependence, Access & VDS

There is a growing shift in HCI research to consider how disability studies frameworks [75, 92, 115, 130], like interdependence [23, 68, 84], might enable a richer understanding of access and VDS. Broadly, interdependence is defined as the mutually negotiated dependencies and collaborations [84, 126]. Feminist disability studies scholar, Alison Kafer, theorized the political/relational model to underscore that disability is a political category that is deeply connected and intertwined with struggles against racism, sexism and colonialism. Disability is also a relational experience because access is shaped by social relations [84]. Through such sensibilities, interdependence enables us to frames access as a relational labor that is built by disabled/non-disabled people, communities and structures [68, 84, 106]. Interdependence complicates narratives of independence as individualized [68, 84] and towards attending to how access is collectively built and sustained. Disability justice activists, who extend and complicate the United States disability rights movement [29, 78] through centering intersectional experiences [29, 51] of disability along the lines of race, gender, and class, have played a vital role in conceptualizing and working toward interdependence. For example, disability justice activists created Sins Invalid which is a performance project that fosters interdependent networks to support disabled people, specifically disabled artists who are also people of color and LGBTQ+ [78].

Drawing from this lineage, HCI scholars proposed interdependence as a useful framework to understand and build access technologies [23, 53, 124]. Bennett et al. conceptualizes interdependence within assistive technology through four tenants 1) focusing on relations, 2) highlighting the overlapping areas of relations and assistance, 3) revealing the labor of disabled people in creating access, and 4) complicating ability-based hierarchies and power differentials [23]. These understandings contrast popular discourses that frame VDS solely as tools to increase independence, rendering Blind and low vision people as "receivers" of help [1, 5, 25, 97] and discounting the many ways that access is mutually built [23, 28]. Within human-based VDS, titles such as "Be My Eyes" [57] minimize and conceal the labor that Blind people perform when using such applications [23]. Through engaging in participant observations, Thieme et al. unpack the layers of interpersonal, fluid negotiations people with visual disabilities undertake to build access *with* people in their networks [121]. Blind people often have to perform additional labor to ensure that lighting conditions are sufficient for VDS to recognize the visual context [9, 80]. In later work, Bennett and colleagues draw from Leah Lakshmi Piepzna-Samarasinha's scholarship on care and interdependence [106] to problematize 'task-oriented' approaches in designing for visual interpretation and call attention to the everyday, mundane and non-innocent, aspects of building access [28]. In recent CSCW work, Vincenazi et al. move away from trying to frame navigation as a 'problem' that AI can 'solve' towards recognizing how AI might play a role in enhancing interdependencies between Blind people and sighted guides [124]. As past work established [23, 28, 124], interdependence is a useful orientation to understand access technologies such as VDS. In our work, we demonstrate how interdependence allows to further understand the opportunities and challenges of obfuscation in VDS.

2.3 Privacy Implications & Harms of VDS

Despite their benefits, VDS have shortcomings and harms. AI systems have drawbacks when it comes to recognizing 'low quality' pictures (i.e. blurry, off-centered pictures, or lighting issues) [67, 83],

requiring Blind and low vision people to undertake extra labor to ensure sufficient recognition conditions [23, 28]. Computer generated descriptions are often framed in an overly confident and deterministic matter, leading Blind people to over-trust system outputs [91]. AI-based VDS are also laden with biases. For example, object recognition data sets are overly populated with objects that are mostly consumed or used in the West [54]. Focusing on racial and gender bias, Bennett and colleagues unpack the harms of AI-generated descriptions on race and gender in terms of misrecognition, unwanted identity disclosure, and reduction, calling for accountability and design consideration to address potential harms that arise for AI applications in accessibility [24].

Both human- and AI-enabled VDS have significant privacy concerns [12, 35, 40, 66, 116]. Broadly, cameras are thought to be one of the most privacy-invasive technologies [14, 87]. VDS privacy policies are ambiguously framed and difficult to read [116]. To gain access in an ableist world that privileges visual ways of being [25], Blind and low vision people have to compromise privacy concerns [11]. This in line what disability justice activist, Mia Mingus, refers to as 'Forced Intimacy' which is defined as "being expected to share (very) personal information with able bodied people to get basic access [..]" [96]. Blind people have called for VDS companies, particularly Aira, to improve privacy practices [3, 58]. This activism led to the inclusion of a feature where users can ask the agent to stop the recording [3, 58]. However, this feature requires users to fully trust that the agent has stopped their recording without any mechanism to cross check that the session is not recorded [58]. In critiquing the discourse around AI applications that are thought to help Blind and low vision 'see', Bennett and Keyes pose a critical question "sight for whom and what gets seen?" to underscore tensions around racial bias, surveillance and misuse (e.g., the potential use of data to train policing technologies) [25].

Prior work focused on classifying and understanding privacy concerns. By analyzing over 40,000 images collected from Blind users of VizWiz, Gurari et al. found that over 10% of these images contained private information [66]. The authors identified 19 categories of private visual information (e.g., credit cards, licence plates, and prescription pills) and demonstrated the possibility of developing algorithms to detect private content. Later work by Stangl et al. extended this taxonomy through interviewing Blind and low vision people, revealing tensions around (un)known disclosures (i.e., private content accidentally apparent in background) and identifying 21 privacy concerns (e.g., social security information or education related documents) [116]. Akter et al. focused on privacy implications of human-generated VDS, noting cases of 'impersonal trust' [52, 113, 123] where Blind and low vision people appeared to trust paid agents more than volunteers [12]. Collectively, these works call for the need to train and build computer vision systems (obfuscation) that are able to recognize contexts and private objects, and blur or redact them if applicable [12, 66]. A major goal of these studies is to inform the development of machine learning technologies [12, 66, 116] and policy [116] to address these established privacy concerns in VDS.

Prior work on VDS has primarily defined and classified private content through the lens of disability. Aligned with disability justice sensibilities [29], VDS should also consider intersectional experiences based on race and cultural background [19, 51]. Our work extends and complicates understanding of private and obfuscation content through attending to cultural dynamics of privacy in addition to disability. Further, we unpack how privacy considerations are dynamic rather than static.

2.4 Obfuscation

Brunton and Nissenbaum define obfuscation as "the deliberate addition of ambiguous, confusing, or misleading information to interfere with surveillance and data collection" in order to resist power imbalances between users and corporate/governmental entities [49]. For example, sex workers often obfuscate their real name by adopting an alias when using digital forms of payment (e.g.,

Venmo or Paypal) to protect themselves from stalking and other forms of violence [94]. Parents obfuscate their children's faces when posting on social media by adding digital stickers and emojis to preserve privacy [20]. To resist automatic takedowns from content moderation algorithms, users who type in Arabic obfuscated social media posts about Palestine by using an ancient Arabic dotless font [16]. Black Lives Matter protesters were advised to obfuscate faces when sharing photos online to safeguard against retaliation and surveillance [125].

In visual contexts (e.g. videos and images), current and emerging strategies include data opt-out mechanisms for users/bystanders [10, 87] and context-aware systems that prevent recording in certain situations (e.g. being in the bathroom) [90]. Visual obfuscation uses transformation (e.g., blur, edge, masking) to enhance perceived or actual privacy. Specifically, obfuscation methods can either be applied to specific regions of the visual content that are pre-defined (partial obfuscation) [15, 73, 90] or are fully applied to the visual content (total obfuscation) [55]. While total obfuscation can greatly enhance privacy, it limits the utility of the content by making it significantly harder to interpret [14]. Past works investigated the use of partial obfuscation through "blocklist" approaches [73, 90] that removes a pre-defined list of objects (e.g. faces) to be removed. However, blocklist approaches are thought to be impractical and partial given the difficulties of accounting for a vast range of contexts [15, 108]. Alternatively, "activity-oriented partial obfuscation" highlights specific regions of interest that are triggered by activities (e.g., a person drinking) and obfuscate everything else [15]. Through conducting a set of experiments that included various scenarios (e.g. bystanders smoking in the background), Alharbi et al. report reduced bystander privacy concerns as obfuscation intensity increases while also noting other concerns such as potential misinterpretation of what might the bystander be doing in the background [15].

Within accessibility-related applications, researchers have explored and suggested obfuscation as a means for privacy preservation. In the context of sign language datasets, Bragg et al. introduce filters to obfuscate the identity of those contributing visual content (i.e., hiding face or full frame) to increase data participation in minoritized communities by providing privacy protections [39]. Kaur et al. used the VizWiz dataset [31] to build "CrowdMask" which is a crowd-powered system that segments and distributes visual contents to different individual workers so that private elements would be detected without being fully viewed by one worker [85]. Overall, obfuscation is thought of as a desirable way to preserve privacy in visual contexts without sacrificing utility. For that reason, a number of scholars working on privacy implications of VDS suggest obfuscation as potential way to address privacy concerns [12, 66, 116].

Despite growing suggestions to develop obfuscation technologies, the perspectives and opinions of Blind and low vision people on obfuscation is unknown. Given how obfuscation in image and video contexts is highly dependent on users' visual abilities to interpret model outcomes [15], it is important to center the perspectives of Blind and low vision people in early stages of developing such systems. Scholarship within CSCW and HCI argues for including relevant social groups within the design and development of emerging AI technologies [44, 109, 127] to construct design and ethical trajectories. Our work aims to inform the design futures of obfuscation technologies with Blind and low vision people by unpacking the potential opportunities and harms of obfuscation in VDS.

3 METHOD

To understand the perspectives of Blind and low vision people on obfuscation technologies within visual description services (VDS), we conducted semi-structured interviews. In this section, we describe our positionality, recruitment approach, and analysis procedure.

3.1 Positionality

This work is led by a team of sighted accessibility researchers and we acknowledge this as a limitation given the focus on the Blind and low vision experience. To reflexively consider our position as researchers doing work with a community we are not a part of, we move away from taking 'empathy' approaches that harmfully seeks to invisiblize and reduce towards recognizing our asymmetries [27]. We follow a feminist disability lens [60] in various direct and indirect instances of this study, including how we understand disability, recruit participants, pose questions and interpret interview transcripts. In this section, we invoke the feminist practice of 'sitpoint theory' [61, 62], a neologism of 'standpoint theory' [72], that builds from traditions of recognizing one's own situatedness and positions of power in research towards explicitly complicating underlaying ableist and normative assumptions [62]. We align with perspectives that define disability as a (socio)political construct that is placed within larger power structures, rather than an individual or medical "deficit" that ought to be fixed and eliminated [60, 84, 106].

At the heart of this work, we're inspired by Alison Kafer's call to critically imagine accessible futures and coalitions [84]. We also learn from and ground our study in *Crip Technoscience* commitments proposed by Aimi Hamraie and Kelly Fritsch [68]. Specifically, we privilege "disabled people as designers and world-builders" and echo the importance of including disabled people in the design and refusal of emerging technologies [68].

3.2 Recruitment & Participation

From March to May of 2021, we conducted semi-structured interviews (N = 20) with adults who regularly use visual description applications and live in the United States. The interviews lasted from 45 to 90 minutes. We posted our recruitment message and screening survey on various social media sites (e.g., Reddit) and the National Federation for the Blind listserv. The recruitment survey included optional demographic (e.g., race, gender, age), vision level (e.g. totally Blind, legally Blind, low vision or self-describe), and types of VDS currently used. If applicable, we inquired about VDS that they had used previously but no longer do so. Over 300 people responded to our recruitment survey. We sent invitation emails to 40 people to interview. Following HCI calls to attend to intersectional marginalized identities [24, 46, 101, 107, 112] and feminist disability studies/justice frameworks [61, 68, 84, 106], we tried to prioritize reaching out to older adults (over the age of 65), people of color, and trans*/non-binary people as these intersections are often not accounted for in mainstream accessibility research. We also recruited participants with varying experiences with visual memory (e.g., totally Blind since adulthood or low vision since childhood) and visual description services (e.g., human-enabled or AI-enabled).

Out of the 40 invitations, 20 people responded to the invitation by consenting, scheduling, and participating in the interview process. Overall, we interviewed 12 women, 7 men, and 1 non-binary person. Participants had diverse visual disabilities: 12 identified as totally Blind, 5 are legally Blind, and 3 are low vision. The majority (N = 9) of our participants have visual disabilities since birth, 4 since adolescence, 3 since adulthood, 2 since childhood and 2 not reported. Out of 19 participants, with age ranges from 20 to 61 years old, the average age was 38 with a standard deviation of 13. One participant did not directly report their age, rather they mentioned being over 50 years old. In terms of race and ethnicity, one participant is both Arab and Asian, two are Arab, two are of Latin/Hispanic descent, three are Black, five are Asian, and seven are white. While only four participants mentioned professional experience with technical accessibility and user testing, we noticed that all participants have a unique expertise in technology and AI/ML that stems from lived experience (as past work affirms [7, 26, 30, 118]). After the interview, participants were compensated

with a $35 (USD) gift card as appreciation for their expertise and time. This study was approved by our institutional research ethics board.

3.3 Procedure

3.3.1 Semi-structured Interviews. We followed a semi-structured interview approach to allow participants to freely talk about their experiences and preferences when using access technologies such as VDS, how they negotiate privacy concerns, and what are their thoughts around emerging obfuscation technologies. The interviews generally encompassed three sections: 1) consent, 2) specific questions about past experiences with VDS, and 3) imagination activity where obfuscation is introduced and participants are asked questions about potential situations where obfuscation would be helpful or harmful and how to better obfuscation. For reference, the interview protocol can be found in the appendix.

First, we obtained verbal consent. Then, we inquired about the current ways participants (non)visually sensemake, asking about specific VDS they use. Specifically, questions 1-6 in section A.2 of the interview protocol aims to uncover these experiences. We noted incidents when participants mentioned negative or positive experiences of using VDS and asked follow up questions. We used these disclosed experiences with VDS in proceeding part of the interview.

The third portion of our interview is referred to as the 'imagination' session where we encouraged speculation on emerging obfuscation technologies (as inspired by past literature [44, 71, 109]). This approach draws from feminist disability and crip studies works [68, 84, 128] that center disabled people in the development of technologies, acknowledging their expertise and creativity as makers and shapers of access technologies. We briefly and generally described the current stage of obfuscation technology if applied to VDS in a hypothetical matter to elicit reactions and thoughts. Before describing the activity, we emphasized that there is no wrong or right answer. We described obfuscation as:

> Let's say, hypothetically speaking, [visual description service participant is familiar with and uses frequently] had a new update where they automatically hide things that are considered to be personal, embarrassing or sensitive by maybe putting a black box, blur effect, or emoji on it so that visual description service providers would not be able to tell exactly what is being concealed. Before moving on, do you have any questions about this scenario?

To avoid priming participants, we did not use terms like 'privacy', 'artificial intelligence', or 'obfuscation' which could introduce potential biases or preconceived notions. Upon describing the hypothetical technology (obfuscation), we asked the participants about their first reactions to obfuscation to help serve as a guiding point for follow-up questions. Building on HCI and CSCW approaches to elicit participant responses and values around emerging technology [34, 47, 109, 131, 132], we then asked about past or future experiences where they might have found obfuscation technology helpful or harmful. Drawing from previously disclosed experiences in second part of the interview, we asked participants to refer back to these moments (e.g., 'remember when you told us you that you were hesitant to use Be My Eyes to help with taxes...') and if they thought obfuscation would make a difference in how they felt. We used these disclosed experiences to situate obfuscation technologies within the participants' personal meaningful experiences. We asked participants to 'think aloud' and reflect on potential tensions and opportunities. At the end of each interview, we wrote a detailed memo. If necessary, we modified, and adjusted our questions to account for emerging themes or improve language for clarity.

All interviews were conducted remotely via Zoom, FaceTime, or phone as preferred by participants. Upon gaining consent, interviews were audio-recorded and transcribed verbatim manually or using transcription services. Given literature complicating the use of researcher selected pseudonyms [48], we gave participants an option to select their own pseudonym or have researchers choose one for them.

3.3.2 Data Analysis. Our approach to data collection and analysis followed a reflexive thematic analysis approach [41–43]. The first author open-coded the interview transcripts and wrote analytical memos, constructing over 50 codes around potential relevant themes such as use examples, privacy, benefits, and harms of obfuscation. All authors discussed the codes and excerpts throughout multiple months, working towards organizing a final codebook that includes 18 defined codes (e.g., benefits of obfuscation and harms of obfuscation). Then, the first author recoded all transcripts according to the final codebook, wrote analytical memos, and continued meeting weekly with the research team to discuss broader categories and themes. Finally, we organized data into three primary themes that capture the ways Blind and low vision people imagine experiencing and interacting with obfuscation.

4 FINDINGS

Our analysis reveals three main themes that detail how Blind and low vision people would like to experience and interact with obfuscation. We report potential use cases for obfuscation and tensions. Findings illustrate the challenges and opportunities, highlighting user needs and suggestions for future obfuscation technologies.

4.1 Obfuscation Use Cases

In this section, we describe key considerations and use cases that participants reported when deciding to obfuscate content. Obfuscation is thought to enable more control over textual materials, manage social impressions and enhance visual description. However, while obfuscation might increase sense of privacy and comfort, participants also discussed harmful aspects that could emerge due to obfuscation when performing complex tasks (such as outdoor navigation).

4.1.1 Obfuscation to Gain Control Over Text. When requesting visual descriptions, participants noted that not everything captured by the camera needs to be described or viewed by VDS, especially when seeking interpretation for selective parts of sensitive data (e.g., financial or medical materials). For example, Tatum told us:

> [W]hen I got my taxes done. [...] I called Aira to get them to tell me what was written on line 11b. [The tax form] had my social security number and all that on there. That wasn't necessary because that wasn't what I was actually looking for [...] They [Aira Agent] were reading that, and I was like, "Oh, I didn't realize it had my social security number and my husband's social security number on our paperwork there." It was papers that went with our tax forms. They don't really need to know our social security numbers.

Tatum told us that as the Aira agent was reading aloud the tax form, she realized that the agent gained access to irrelevant private information (social security number) beyond the main reason she requested visual description (knowing the components of line 11b). *"I think that an application [obfuscation] like that would have been excellent in that situation,"* Tatum emphasized. Obfuscation might help Blind and low vision people gain control over visual disclosures by detecting and filtering specific textual content based on user visual description needs while allowing other regions of interest to be legible for VDS such as Aira.

Many participants also shared this sentiment on how obfuscation might be a great solution to providing an increased sense of control, security, safety, and comfort when using VDS in their everyday life. Remembering a time when he lived alone and needed to use VDS to read sensitive materials, Ahmed shared with us:

> To read things, I used to use Seeing AI more. And I would open any letter to see what's going on, but I wish I knew that there is an option [like obfuscation], and if it can be deployed as soon as possible. That would be much better. It would help me, at least in my privacy. I don't want my information everywhere because that happened to me 10 years ago. Somebody stole my social security, and my tax return. And basically, it took me a while to fix all of that.

Drawing from his past experience with identity theft, Ahmed explained that obfuscation might help provide more control, like obscuring social security numbers when using VDS to read through sensitive material. Simran, who works in the clinical field and often uses Seeing AI for textual documents outside of work, told us *"But if the app is or may introduce [obfuscation], I would be relaxed to use the app more so I know that my clients' information will not be shared."* Obfuscation resolves anxieties around sensitive textual data being, as Ahmed puts it, *"everywhere,"* and potentially viewed by others such as agents/volunteers, data servers admins, or harmful actors in cases of data breach. Prior work establishes that the data handling practices of visual description applications are unknown to users [116]. Some participants raised concerns of over data breaches and potential security incidents. J commented that *"we can expect places like Microsoft or Google to occasionally be breached [...] We don't know about Aira's servers, they're probably using AWS or something which means they are covered by Amazon, but we don't know that."* Ruth also noted concerns around *"[i]n this day and age of so many things getting hacked, and so much data being compromised."* Consequently, obfuscation, through allowing for control over what is disclosed and shared with VDS, could provide *"assurance that no one's going to see something that you don't feel comfortable with"* as Emma told us.

Unpacking further use cases of obfuscating textual materials, Danielle told us about an incident where selectively obfuscating specific regions of a textual material would have been helpful in preserving privacy. After returning back home from a medical procedure and carrying a pile of discharge paperwork, Danielle needed to use Be My Eyes, a human-based VDS that uses volunteers to provide description [57], to identify which of these documents was the excuse letter to then send to instructors. She explained that some of these textual materials included sensitive information such as *"diagnosis and the procedure that was done and the dates and any medications that had been prescribed."* Danielle pointed out that these were not necessary details for Be My Eyes volunteers to determine which of one of those papers was the excuse letter. Instead, simply highlighting the header of the documents and obfuscating other sections is sufficient enough to distinguish the excuse letter. Jessica shared an example from her Blind friend who often needs to use VDS for identifying sensitive materials. Jessica recalled *"one of my buddies, he smokes marijuana and so he needed to know the size of the bag."* In most cases, drug labels include relevant information such as dosage and expiration dates. To get the requested description (e.g., size), VDS does not need to view what might be in the bag or container as this information is likely include in a label. Obfuscation could enable more control by maintaining relevant materials to the description process while obscuring other sensitive details that are not of interest to the user's main visual description request.

Selectively obfuscating specific sections of textual materials allows for an increased level of control, security, and comfort when using VDS. Participants recalled use cases for obfuscating specific regions of tax forms, medical documents, drug labels, and financial letters. Through gaining

control over what types of information are disclosed to VDS, obfuscation could alleviate worries over data breaches and enhance user privacy.

4.1.2 Obfuscation for Impression Management. Some participants talked about how obfuscation could perhaps mitigate some of the stigma that Blind people experience when unwanted background details are captured. Given the pervasive nature of cameras, many private and irrelevant elements might be included in the background. Blind and low vision people adopt VDS in various situations beyond identifying or filling out documents. For example, previous work have explored how VDS is used in and for daily activities, like shopping and traveling [12, 50, 121], which our participants also emphasized. Within these use cases, content that ranges from less private (e.g., a pile of cookbooks) or more private (e.g., a person in the background using the bathroom), might be apparent in the background, causing embarrassment or stigma. Jessica pointed out that *"it could be that maybe a person in the background or in their environment is doing something that the Blind or visually impaired person didn't see and that it could be captured [by VDS]."* Sophia explained that sighted volunteers or agents might pity Blind and low vision people for unintended background disclosures, *"they are gonna think 'Oh, dear, oh, there, look poor thing she's Blind. So she doesn't know that whatever is on the lying on the bed is there'"* As described in prior work [12, 116], background disclosures of content pose a high privacy risk for Blind and low vision people and increase burden of impression management (e.g., making sure your room looks tidy and up to social expectations) [63, 64]. Thinking of a past experience using Be My Eyes, Ruth told us:

> I can't see the expiration date, and I am holding the carton of milk on my counter and I'm thinking, "Gosh, my counter is really disgusting, it's really messy. I really wish they [Be My Eyes volunteer] didn't have to see this.

Ruth felt embarrassed that Be My Eyes volunteers were able to view her kitchen counter in a far from ideal stage, creating tensions with how she wishes to manage social impressions. Obfuscation has the potential to limit the capture of unwanted details in backgrounds. Specifically, instead of including all that it is in view, obfuscation provides control over spotlighting relevant content (e.g., milk carton) and obscuring other details such as messy counters. Obfuscation could afford a sense of control over background disclosures, reducing burden of impression management and stigma when using VDS, especially human-based VDS.

4.1.3 Obfuscation to Enhance Visual Description. Obfuscation could also lead to improved description quality. Particularly, obfuscation could help make the description process better by narrowing the scope to focus on a specific region of interest instead of capturing every single aspect in the background. For instance, RB told us that *"sometimes you need assistance in the restroom area, looking in the toilet bowl and those kinds of things, and if it is a public restroom you don't want your [Be My Eyes] volunteer to see other people doing their business there."* For that, RB speculates that obfuscation might aid in privacy management and help the visual description process:

> I'm just imagining from a sighted person's perspective, looking at the screen, that it's dark, dark, dark all the time, and all of a sudden, while the Blind user is moving the camera, and the moment it detects the toilet bowl I think that potentially would help the volunteer to get rid of all the noise around it and just be able to guide the Blind person much more quickly.

Specifically, RB notes that obfuscation would act as a block and only enable the view once a toilet stall (the object relevant for visual assistance) is detected. At that point, Be My Eyes volunteers would be able to provide visual guidance on where the toilet is located. Obfuscation removes any noise that might distract volunteers while preserving the privacy of bystanders. Similarly, Saad shares that *"it would be nice to blur everything out and focus on the subject… before you call [...]*

So you say like, 'Oh, okay, do you want to focus on the computer screen, or a screen in general, or a microwave' or something of that sort." Obfuscation could aid in controlling background disclosures by solely highlighting specific objects of interest and obscuring everything else, enhancing the visual interpretation process.

Numerous participants commented on how VDS is currently limited in their descriptive capacity. In fact, our participants detailed that they are actively involved in guiding the visual description process to make sure it goes smoothly. Sophia told us about her experience using Be My Eyes:

> Okay, so you call and you say to someone: "please, can you tell me what this is?" Okay, like you're showing them a package. And the first thing they tell you "Oh, it looks like.. it looks like it is.." and I'm like "it looks like"? Wait.. I mean, of course I'm not rude. I'm not gonna say that, you know, but I'm like, no, you have to tell them: "Please, can you read to me what this is?" [...] So, you got to be specific, you got to know what to ask.

Hasnain also expands *"I have to explain what I need their help with, which is not a big deal. But the issue is that when people give me these vague, too wide directions like, 'Oh, it's over there,'"* Our data reflects, as discussed in prior work [23, 28, 44, 121], that Blind and low vision people do engage in labor to build access rather than being passive recipients. In using Human-based VDS, Blind and low vision people labor by communicating with volunteers/agents and detailing what exactly needs to be described and to what extent. Obfuscation, through controlling background disclosures, could filter out irrelevant details and improve description quality.

4.1.4 Potential Harms. Participants noted harmful implications when using obfuscation. Some participants noted there are tensions with obfuscating texts and needing to use VDS to recognize private materials in its entirety without obfuscation. In thinking about a situation where obfuscation where RT might want to read the label of a pill bottle, they told us:

> I can't help but think that [obfuscation] would be really irritating because I'm probably pointing the camera at my pill bottle to read it. Then if it's like, we privated this because it looks like it's personal information. It's like, "No, I need you to read this for me."

In this case, obfuscation would automatically and annoyingly obscure the entire pill bottle, disregarding the RT's wishes to read the label. Additionally, Clara told us *"I don't know my bank number off the top of my head, but I might want it to be read it out loud to me."* It would harmful if obfuscation automatically blocks information such as bank numbers. While obfuscation might help in gaining control over textual materials (e.g., financial and medical information), there are moments in which participants did not want such information to be obfuscated.

Participants questioned the obfuscation algorithm's capacity to recognize context. RT told us *"the [obfuscation] AI isn't going to know if you're trying to look at something for yourself or it just happens to be a background detail."* As RT pointed out, determining what might be merely a tangential background detail or an important element to be described is a difficult task for algorithmic systems like obfuscation. J also added *"when is it okay and when is not important to hide a face? or when someone is half turned from you and is in side profile, so it can't see it very well. Or, you know, moving people, shadows and light, depending on the day and time of day, and was in the environment. It all just seems so... so many failure points."* Indeed, the accuracy of visual systems, including obfuscation, depends on environmental conditions that are hard to control. These include lighting conditions and bystander position. While obfuscation systems might be able to easily recognize bystanders that are looking directly into the camera, it is likely difficult if they are turned to a side. Some participants were not convinced that obfuscation algorithms would be capable of recognizing

detailed contextual information to improve the quality of visual descriptions, raising numerous factors that lead to misrecognition (e.g., shadow, position, and light).

Obfuscation might also obscure details that are relevant to visual description. Martha commented that *"it could be something in the environment that I want the [Aira] agent's help with but if it's hidden, then we have to go through this whole thing of like how to hide it or move this way or move that way so they can see it or whatever. It just doesn't seem efficient to me."* Obfuscation might not be an efficient way of enhancing visual description because it could omit regions of interest to the visual description process. Removing important background information might not be useful for enhancing visual description. Rather it could be harmful, burdensome and potentially dangerous. In the case of navigation, obfuscation is likely to be distracting and could lead to safety risks. For example, David told us:

> if you're walking around and all of a sudden [...] you're following some navigation and you and it senses something in the environment that it deems as inappropriate or sensitive and it blurs it out but also then includes the help you're trying to get. All of a sudden an agent can't see a street sign or something because it is actively being occluded. That's that's definitely going to be a dangerous problem.

Using obfuscation in complex tasks like navigation could lead to safety issues. In David's example, agents in human-based VDS might lose important visual cues to guide the navigation process leading to potentially dangerous consequences. Similarly, Jessica told us about how VDS has help her avoid bumping into obstacles and other passerbys as she navigate. Recalling a specific incident, she told us *"I had gone to vote, and you know how messy voting has been since COVID, and all of that. And so what happened was, I used Uber to go to put my ballot into the ballot box [...] I turned the phone to the car and said to the [AIRA] agent, this is the car I need to return to and she said okay[...] she was all along the way warning me of, 'Oh, you're going to hit this.'"* When using obfuscation for complicated tasks like navigation, it could lead to the loss of important contextual materials that are relevant. This results in potentially dangerous situations like running into a passerby or upcoming surface-level challenges like potholes and curbs.

4.2 Shaping Obfuscation

Participants underscored various suggestions that are critical to the development of obfuscation. Specifically, these revolved around enacting agency through choosing obfuscation content and determining obfuscation decisions.

4.2.1 Choosing Obfuscation Content. Participants wanted avenues to choose what type of content would be targeted and optimized by obfuscation systems. Given their everyday interactions with AI-enabled VDS systems, some participants recognized the importance of datasets in constructing systems like obfuscation. J emphasized that *"AI takes time, AI learns based on input and that input needs to be curated by humans usually, at this point. Because otherwise, you know, bad data in, bad data out."* Specifically, participants questioned the inclusiveness and quality of obfuscation datasets, emphasizing the concerns for bias. David pointed out that privacy is nebulous and difficult to define as it is *"very subjective because maybe it could be things like a sensitive adult nature, or an explicit nature, it could be again, legal or financial data."* Clara also added *"maybe someone doesn't want their, the child or dog's name like out out there. It doesn't have to be something as important as a social security number. It could be something less important to someone else. Everyone has their own definition of privacy and what they want hidden."* While some participants admitted that there are universal privacy considerations shared by nearly everyone, they echoed that there are some concerns that are subjective and unique.

On that thread of thought, David critically asked *"who's making that decision? Who's making... who's making the moral decision as to what what constitutes something as being sensitive?"* Notably, none of our participants wanted VDS companies to impose a limited set of content that Blind and low vision people could obfuscate. Rather, participants wanted to decide what type of content should be obfuscated. Some pointed out the potential for community-based engagements with Blind and low vision people to collectively brainstorm and discuss what content should be included in obfuscation datasets. Danielle stated:

> [B]efore you roll [obfuscation] out, you send out a list to the public [...] I think that [obfuscation developers] should allow the public to also put their input in and based on what kind of input they get, they may adjust that list accordingly. But before they make it set in stone, they should really engage the public in that decision making process.

Some participants highlighted the difficulties of understanding privacy and obfuscation through a community-based lens because the Blind and low vision community is not homogeneous; privacy considerations often intersect with other identity factors like race/ethnicity and religion. Put succinctly by RT, *"consulting with one Blind community isn't consulting with all Blind communities. There's just such a wide range. What if you consulted with the largely Mormon demographics of one Blind community, and then you just completely skip out the Muslim Blind community or the atheist Blind community."* Indeed, a number of participants expressed how their privacy concerns, which are largely based on their cultural and ethnic background, could be left out from obfuscation datasets. Speaking from his own cultural experiences between the United States and the Middle East, Saad stated that *"in the Middle East, there are more concern about their families, especially towards females and stuff. On the other hand, in the US, for example, medication is big deal. So people in the US consider medication a very private thing whereas in the Middle East it is not a big deal."* Privacy behaviors and decisions stem from cultural and social factors. Sophia reflected on her own privacy concerns, *"what might be totally fine to an American person. I mean, to someone who was born, raised, and grew up here, might be quite sensitive to me as an Arab woman."* Also, Simran, who uses VDS to describe pictures of scenery, told us *"if I'm showing a picture of someone kissing it is considered embarrassing in my culture. No one should be kissing in front of other people. But in Western countries, it's kind of very normal so that wouldn't be considered as embarrassing."* Public display of affection are considered based on cultural norms, Simran and other participants brought up examples that do not align with popular, Western, understandings of sensitivity and privacy. Overall, participants emphasized that some privacy concerns that are prominent within their communities might not be included in the types of content privileged by obfuscation systems. This is often the case as dominant computer vision datasets are biased toward Western countries [54].

4.2.2 Dismissing and Consenting to Obfuscation. During our interviews, a majority of our participants objected to automatic obfuscation decisions that do not allow users opportunities to interject through dismissing/consenting obfuscation decisions. Some referred to automated approaches as intrusive and unfair. RT told us:

> The function of [VDS] is to let you see what everybody else is seeing. Even though it's an embarrassing kind of thing, if that's out where people with two eyes can look at it, it's really unfair to take that away for me, even if it's information that I'm like, "I didn't want to know that." But it's still information that everybody else has access to, and depriving me of access to that information is a kick in the teeth. I already get that from basically everything else. It would really suck if my accessibility app [VDS] was doing the same thing to me.

Participants wanted a choice in actively determining what gets obfuscated or not. RT asserted that even if obfuscation was applied to something they did not want a description of, they want to be able to consent or dismiss obfuscation. Otherwise, as RT noted, automatic obfuscation might lead to equity issues and goes against the core functions of VDS: to provide visual descriptions. RT emphasized the importance for accessing content that might be detected for obfuscation, noting that occluding such information is exclusionary and in line with other forms of oppression and ableism that are experienced everyday. For that reason, it is important that the design of future obfuscation systems allows users avenues to dismiss/consent to obfuscation decisions. Fully automating obfuscation decisions, without enabling users an opportunity to consent or dismiss, is harmful.

Even if automatic obfuscation only targeted content that might be universally regarded as private, that could be problematic. As touched upon in section 4.1.1 and past work [11, 12], Blind and low vision people often need to use VDS to recognize materials that are traditionally thought to be private such as medical or financial forms and obfuscation should not hinder from making these decisions. Gabriela presented us with a thought-provoking hypothetical situation that challenges assumptions about what might be rendered as private and under what condition, she told us:

> So let's say it's a picture of a naked child. And I'm going to use this example because what happens is when you think of a picture of a naked child, automatically you're like, "No, absolutely not." But what if there is concern about a child getting hurt? So if I was a Blind mom [and I] took a picture of a child, either my child or a child that I was, I don't know, babysitting because I had speculations that this child was getting bruised or something like that [...] So I think that, once again, it should be a decision that the Blind person makes because what may be sensitive and personal for someone else, may just be a matter of identification and reassurance for a Blind person.

Gabriela worried that obfuscation systems might not recognize the complex instances where she needs to negotiate privacy concerns to achieve peace of mind. Particularly, she noted that obfuscation should not be built on the *"automatic assumption that something is indeed personal or sensitive, because it may be personal or sensitive information that the Blind person needs to access."* Instead of automatic obfuscation approaches that do not recognize complicated privacy decisions and access needs, obfuscation should integrate consent/dismissal mechanisms.

4.3 Feedback from Obfuscation

In order to realize the desires of section 4.2 in shaping and enacting agency over obfuscation systems, participants noted the importance of receiving feedback such as description of content flagged by obfuscation. Further, participants report opportunities to reconcile tensions around trust and obfuscation misrecongition.

4.3.1 Describing Obfuscated Content. Obfuscation systems need to describe targeted content. Participants spoke at great length about the importance of knowing what obfuscation systems detected as private. RT shared that:

> Having ADHD, I can say immediately as soon as something is being privated [obfuscated], my first thought is, what is it? I want to know what that is. That's going to distract me from whatever I was doing because it's just like, what's so bad that I can't see it? Now I want to know.

Participants emphasized the significance of knowing what is the content flagged by obfuscation systems. Otherwise, as RT summarizes, it could distract from the visual description process. Providing a description of what obfuscation systems highlighted as private is critical to the development of obfuscation systems. It is also necessary to achieving consent and dismissal which is of value to participants as we establish in section 4.2.2. According to J, designers might implement description, consent, and dismissal with a series of prompts:

> With an AI [obfuscation] system like this I would prefer it to go "something in your images [is] being hidden. Would you like to see what it is? What's the issue? What are we detecting that we think is this way?'" And then you could say "yes that's an issue" or "no that's not."

In addition to providing description for the content targeted by obfuscation and consent/dismissal, J also imagines opportunities for obfuscation systems to describe *why* such content was detected. This might help Blind and low vision people understand system-level rationale that goes into obfuscation.

Participants explained how description feedback from obfuscation might be helpful **prior** to interacting with VDS. In reflecting on a past experience, Gabriela told us that describing obfuscated content might be as follows:

> I would like for it to be phrased in a way like "I detected the possibility of…" then, that way, the Blind person could be like, "Oh, my God, I didn't put this away." Because that could happen. That could totally happen. One day, I had not realized that I left my packet of birth control pills on top of the water filter, and I had spent the entire morning looking for it. And I was just like, "Where are they? Where are they?" Imagine now that's usually the spot where I call the [AIRA] agent.

Gabriela notes the potential for obfuscation to be used prior to starting a call with a human-based VDS (such as Aira) to give her the opportunity to consent to obfuscate the described content (in this case birth control) or dismiss and physically remove the object from camera's view. When obfuscation systems describe the content, it could limit any potential distracting curiosities and it allows Blind and low vision people to make informed decisions around consenting to or dismissing obfuscation decisions. In the case of AI-enabled VDS, Clara also imagines the interaction to go along the lines of:

> Okay, so in the case of like Seeing AI if it scans the document first, and then it reads it aloud to you, it could pick it up during the initial scan, and then maybe a dialog box could come up saying 'some private information was detected during this scan. Would you like it to be read aloud or blocked?'

In Clara's conceptualization, users are asked if they would like to have that detected object for potential obfuscation to be described to them prior to using VDS. Instead of explicitly describing the targeted content, as in Gabriela's example, Clara notes that obfuscation ought to broadly describe the content as 'private information' and then leave it up to the user to decide subsequent actions.

Describing targeted content might also give Blind and low vision people an opportunity to obfuscate certain details **after** using VDS and before visual data is potentially stored in VDS servers. Specifically, David told us:

> if you use [obfuscation] to inform the user that there may be sensitive subject matter in the photo before you send it into like a server or machine learning database. It's like you have an image, you don't know what it is when you are try doing recognition on it. But it turns out to be like an adult photo or an explicit

> photo or something that has like your credit card information on it and getting alerted before it gets captured.

As David explained, a user might try to recognize a document and accidentally find out that it contains private information after it has been recognized with a VDS (this is similar to Tatum's experience that we described in section 4.1.1). Even after recognition, obfuscation presents an opportunity to notify and describe the private element to Blind and low vision people, giving them an option to block private elements before visual content are migrated to VDS servers.

Receiving descriptions of obfuscated content while using human-based VDS is difficult. The past section uncovered opportunities to obtain feedback from obfuscation before and after using VDS. Within these, we note a range of preferences on to what extent should that detected content be described. Some preferred concise and vague description such as 'private content' while others wanted specific descriptions (e.g., pill bottle). Feedback **during** human-based VDS presents unique challenges as it requires interacting with people (e.g., agents or volunteers) who might be taken aback from obfuscation descriptions. Some participants told us that full, spoken, descriptions of obfuscated content might be cognitively burdensome. Olivia said having a detailed spoken description of a potentially obfuscated content (e.g., we detected a credit card) *"would be jarring. Like, 'wait, what is this?'"* Ruth reflected *"it would probably be distracting, both to the person that's doing the [visual] description, and to the user, because the user is depending on what the volunteer says."* While a detailed, spoken description of content flagged for obfuscation is important for increasing transparency and gaining consent, it might lead to distractions and safety risks especially in the case of navigation as noted in past section 4.1.4. Hasnain discussed issue of detailed spoken descriptions, distraction and navigation, *"[using VDS] when I'm walking and there are certain visual cues that, if I was not listening and abiding to them, I would have gotten injured."* Spoken feedback from obfuscation might divert user attention from listening to human-enabled VDS agents or volunteers, leading to potential injury. Due to the problem of increased distractions, Danielle discussed the possibility of using audio alerts instead of fully describing obfuscated content. She expanded on this thought:

> Maybe a chime. A chime would be... A special chime for this is an alert because it's detecting something that should have been not spoken, that would be really good. Because the chime is not going to be as distracting.

Describing obfuscated content is important for Blind and low vision people to actively negotiate with obfuscation. However, full spoken descriptions pose potential harm because they are distracting. In essence, changing the description modality from spoken description to simple audio, customizable, alerts (e.g., chime) could help decrease any cognitive overload when attempting to obfuscate content while receiving the visual description.

4.3.2 Tensions and Reconciliations with Interpreting Obfuscation. Being able to interpret the obfuscation process is a frictioned, yet important, feedback that participants emphasized. Misrecognitions and errors are inevitable when dealing with systems such as obfuscation; users must be able to understand and interpret system outcomes. As Martha puts it, *"technology is just not perfect."* Participants highlighted tensions with trusting and confirming if obfuscation occurred correctly. Simran questioned, *"[s]ay for example, if I'm taking my credit card picture, [obfuscation system] tells me what the credit card numbers are [...] But how would I know that you [agent or volunteer] were blocked from seeing my numbers?"* Ruth also added *"there's also the reality that the folks who use it are either Blind or have low vision, and they wouldn't necessarily know what's going on. So they think it's blurred, but maybe it isn't actually blurred, and they don't know it because they can't see it."* Obfuscation demands a level of trust because there is no affordances that allow for non-visual interpretation and confirmation. Collectively, participants acknowledge that technologies, especially algorithmic

systems like obfuscation, are error prone. Currently, the only way for users to interpret such results is through visual sensemaking (i.e., seeing obfuscation outcomes) and that excludes Blind and low vision people. David expanded:

> [T]he only way to assess if it's actually working is if someone sighted can take a look. And say, 'yeah, it's actually being blurred' [...] we can't inherently trust the software as it is right now. So it'd be really difficult if not impossible to make this determination that it's actually working correctly.

Past work suggests the addition of confidence ratings in computer generated descriptions allows for transparency [91]. When exploring the addition of error percentages to confirm the obfuscation process, participants largely found the idea of them not useful. Tatum said *"I don't think the percentage part of it would really matter that much to me."* Adding to that, J told us *"Sometimes [percentages] are vague."* Percentages do not seem to help users make better decisions. Error percentages might even cause worries as noted by ESTP, *"the percentages might scare somebody a little bit more. I mean, there is no software comes with this is how much percentage is that, you know, but… So the phone doesn't say 'we're 80% sure this iOS update is good' you know it doesn't say that. It's just download, assume that it's okay."* These reflections underscore the importance of exploring metrics beyond quantitative measures to address issues of accuracy and confirmation. In essence, percentages did not seem to be a meaningful way to (non)visually confirm the obfuscation process.

Alternatively, many participants emphasized the need to establish safety protocols *when* (not if) such incidents of error happen. As a first step, Blind and low vision people should be informed about errors in obfuscation systems. Xavier told us: *"So [users] have the right to know exactly what happened. And if there was a problem [with obfuscation]: How was that problem solved [...] And it's fair to to expect this. Especially if, you know, [Blind and low vision people] look for these services [VDS], as a way of been more independent."* Participants valued knowing about systems errors and how VDS would respond to such occurrences.

When thinking about how to best approach error in obfuscation, participants spoke about the complexity of data collection processes. While many pointed out the importance of collecting data from obfuscation for quality assurance, participants acknowledged its potential harms. David pointed out:

> This kind of funneling us into more of like a Catch 22, where they need to know why [obfuscation] was glitching. But they can't look at why it was glitching. Because it might be exposing something sensitive.

While it's important for VDS companies to collect and review data where system errors such as misrecongition take place, it poses privacy and security risks for Blind and low vision people. This is the "Catch 22" that David notes. As a way to address such tensions, Clara said *"[VDS] could let me know that their [obfuscation] software wasn't working, and they could give me an option as to whether I wanted it deleted from their server or not."* Ahmed, in thinking about his use of voice assistant devices, also told us: *"But if there is an option to say, 'Okay, load this, don't load this,' yeah, that would be fine. Because let's say with Google Home, and Alexa, there is an option, where you can go on the cloud, on Google Assistant, or Alexa app, and delete all your recordings."* Giving Blind and low vision users the option to send such data, where obfuscation systems might have failed, to be stored and analyzed by VDS is a potential solution to conflicting interests around data collection and error.

Overall, participants wanted protocols and procedures in place to ensure that when obfuscation makes a mistake, they would be notified of the steps VDS is going to take to ensure the safeguarding of their data. Participants also speculated about ways to have more control over their data such as allowing for more choices on the deletion and archival of specific materials.

5 DISCUSSION

To summarize our findings, we uncovered a variety of obfuscation use cases (e.g., obfuscating selective regions within sensitive documents). Participants report that obfuscation might be useful in enhancing the quality of visual description while noting potential dangers when obscuring details in complex tasks such as navigation. With an orientation toward developing future obfuscation technologies, our analysis emphasizes that participants wanted to be actively involved in the obfuscation process through choosing obfuscation content, dismissing/consenting to obfuscation decisions, and receiving feedback from obfuscation systems. Participants echoed the importance of safety protocols for when obfuscation misrecognition occurs, signaling opportunities for VDS-level remediation such as options to delete visual data where obfuscation was flawed.

Building from our findings, we propose that interdependence [23, 28, 84, 106] is a generative framework to conceptualize and design for obfuscation in VDS. First, we revisit our findings with a focus on interdependence. Then, we provide design directions that attend to interdependence in obfuscation.

5.1 Rethinking Obfuscation Through Interdependence

Findings highlight a disconnect between popular trends in obfuscation research and the needs of Blind and low people. Our analysis revealed that participants opposed fully automated obfuscation approaches. Rather, participants wanted to be actively involved in the obfuscation process. Interdependence, as theorized by disability studies/justice scholars and activists, captures the interplay and negotiation between actors, communities, environments, and structures to build access [23, 28, 68, 84, 106]. That is, interdependence centers mutual *relationships* towards a shared goal [28, 68, 106], more closely reflecting how our participants imagined obfuscation. In HCI and CSCW, interdependence has been adopted in various ways such as for revealing the invisible labor of Blind people in collaborative writing environments [53] and enhancing collaboration between Blind people, sighted guides and AI systems for navigation [124]. We take inspiration from tenets proposed by Bennett et al. [23] to underpin how interdependence informs obfuscation through 1) complicating privacy needs by considering its connection with access and identity, 2) uncovering and paying attention to the labor Blind and low vision people *already* perform with VDS and 3) emphasizing the importance of safeguards when error occurs.

5.1.1 Complicating Privacy Concerns. Privacy needs and decisions are intertwined with access considerations. Interdependence understands access as dynamically shaped by the relationship between people and social and material structures [23, 28, 68, 84, 106]. Notably, the lens of interdependence affirms that disability and access needs are not fixed in time and space; rather, they are dependent on a wide range of factors [23, 84]. Corroborating our findings on access and privacy behaviors, past work illustrates that Blind people often need to compromise privacy concerns to gain access to sensitive information (e.g., paper-based medical documents) [11]. In opposition to automatic obfuscation approaches that might immediately block content deemed as private [66, 76], our participants described how their privacy calculus dynamically shifts according to their access considerations. Consequently, it is difficult to classify a certain type of content as 'inherently' private and thus subjected to obfuscation at all times because access and privacy considerations vary. For example, recall Gabriela's hypothetical of needing to use VDS to assess a child's injury. Automatic obfuscation would likely be unable to discern nuanced privacy decisions that emerge with access needs.

Interdependence allows us to grapple with capturing context in AI systems such as obfuscation. Past work aims to identify private contexts when using VDS [12, 66, 116]. Even if automatic obfuscation systems would 'contextually' operate (i.e., recognize the unique privacy considerations),

our analysis emphasizes that privacy and access needs are dynamic and continuously changing based on individual experiences. Understanding and accounting for all possible contexts is challenging, if not impossible. As Dourish argues, context "slips away when one attempts to define it" [56, pg. 13]. Contextualizing obfuscation techniques could lead researchers to overgeneralize limited cases, leaving out important privacy and access considerations. While some participants wanted to obfuscate objects such as financial materials, others highlighted that they might need to use VDS to recognize this context. Here, we note an opportunity for designers to move away from fully automatic obfuscation systems and consider mechanisms (e.g., consent/dismissal avenues) that shift agency and decision making to Blind and low vision people based on unique access considerations. Obfuscation systems must recognize how privacy decisions are informed by access needs so that these systems do not become a barrier. Further, efforts to contextualize obfuscation systems can be redirected towards understanding what makes a particular object private. Beyond the popular total object obfuscation that detects and blocks specific objects thought to be private [66, 73, 102], findings also reveal a need to develop granular approaches to obfuscation that enables obscuring specific regions in the object (e.g., obfuscating everything in the document except for the header needed for the description task). Dynamic negotiations of privacy recognize that while a specific document or a pill bottle is traditionally thought to be private, Blind and low vision people might need to recognize certain subregions within that content (e.g., dosage). This indicates that researchers should develop systems that enable Blind and low vision people to obfuscate specific elements within an object instead of total object obfuscation.

Participants surfaced concerns that obfuscation would fail to recognize (and respond) to their privacy calculus. Many noted that privacy is subjectively defined, often interacting with identity aspects such as race/ethnic background. In disability justice literature [23, 29, 68, 106], interdependence is conceptualized through a community-based lens that affirms the different networks of solidarities between people to build access. Interdependence, as rooted in disability justice, also acknowledges how the experience of disability varies along the lines of race, gender, and sexuality [23, 29, 68, 95]. In writing about interdependence and community, Mia Mingus, who is a writer, educator, and trainer of transformative justice and disability justice, tells us "[...] disabled people are not only disabled: we are people of color, we are all different genders and sexualities, we are from different class backgrounds and cultures, we are survivors, bystanders and offenders—we are human" [95]. That is, rather than reducing disability to a single axis, disability justice embraces intersectionality as a core tenant [29, 51] to recognize how access is constructed and shaped by identity factors beyond disability (e.g., race and gender).

Turning back to obfuscation and VDS, participants expressed concerns over having their privacy concerns erased by obfuscation if merely foregrounding disability (e.g., Blindness) without considering how other forms of identities interact and construct privacy decisions. For instance, recall Sophia's concerns about how her privacy considerations as an Arab woman might be left out from obfuscation systems. Our participants' concern over a lack of representation is extremely valid. Popular computer vision datasets are not neutral [104, 110]; they carry various exclusions and inclusions. As we know from past work, computer vision datasets often have a Western and white bias [54], creating serious representational issues for those pushed to the margins. Obfuscation datasets ought to critically consider how privacy concerns and behaviors are shaped by experiences along the lines of race, gender, and class in addition to disability. Future work could ethically explore the unique privacy and obfuscation concerns of additional marginalized identities such as Blind and low vision people who are political activists [93], sex workers [13, 94], queer/trans [33, 89], refugees [81], undocumented/stateless [65], and incarcerated [103].

5.1.2 Placing Obfuscation Within the Labor Blind and Low Vision People Already Perform. Interdependence highlights the labor taken up by Blind and low vision people in creating and building access [23, 28]. Blind and low vision people are not passive recipients of help; they contribute to the work of access. As our findings illustrate, Blind and low vision people work *with* VDS to obtain visual description. For example, participants would actively communicate with human-based VDS to interdependently produce visual descriptions, guiding sighted agents/volunteers towards what needs to be described and how. As noted in past work [9, 28, 80], Blind and low vision people also put in labor to position documents for optimal AI-based VDS recognition, making sure the image is not blurry and is correctly aligned. It is important that emerging obfuscation systems recognize the work already performed by Blind and low vision people to build access and design systems that align with how VDS is used.

By foregrounding the labor of Blind and low vision people in co-creating visual descriptions, we uncover opportunities and challenges with obfuscation. Opportunities include how obfuscation could be used to spotlight instead of block certain elements to help guide the description process. Through spotlighting what is intended for recognition and obfuscating everything else, VDS providers have more visual clarity on what ought to be described while minimizing labor. Corroborating past work, we found that some participants also engaged in the burden of impression management when using VDS [12]. For instance, recall Ruth's desires for approaches that block Be My Eyes volunteers from viewing messy details of her kitchen. Obfuscation may help in alleviating the pressure of maintaining impressions through spotlighting and blocking specific elements from the view of VDS. We extend past work [12] that suggests resolving burden of impression management through obscuring private content based on who is providing description (e.g., crowdworker or friend) through considering how obfuscation can be used as means to spotlight objects of interests.

More significantly, major challenges arise when thinking about feedback from obfuscation systems. Most feedback from visual systems, like obfuscation, relies on vision and is thus inaccessible. Participants acknowledged the importance of knowing what content is flagged for obfuscation and having agency to dismiss/consent obfuscation decisions. Still, many pointed out that receiving a full spoken description of content targeted by obfuscation systems could lead to further cognitive labor and overload. Receiving obfuscation descriptions is important for achieving informed consent [77], yet it is difficult to integrate into VDS. It is likely to disrupt the flow of interaction between Blind people and VDS providers, leading to communication barriers and even potential financial loss because some VDS require payment [12]. Communicating feedback from obfuscation systems poses a challenge that could even lead to dangerous outcomes as evidenced by our participants' anxieties to use obfuscation in complex tasks such as outdoor navigation. Our results revealed participants' worries that obfuscation description process would lead to negative and harmful implications. It is important for future work in obfuscation and VDS to understand and uncover the specific concerns about obfuscation descriptions when used for complex tasks, like navigation, starting in safe and controlled environments (e.g., in-lab settings).

5.1.3 Establishing Safety Measures for Obfuscation Mistakes. Many participants raised feelings of uncertainty and unknowability on interpreting obfuscation outcomes, detailing worries over obfuscation's ability to meet its promises. Foregrounding sight as a way of knowing, computer vision systems are sometimes framed as transparent because it is assumed that people can make sense of the system by seeing the outcomes. In the emerging area of human-AI interactions, designers are often asked to "show" users model pitfalls through visualizations [17]. However, transparency often goes beyond 'seeing' [18]. Critical scholars have critiqued such limited notions of transparency, arguing that accountability and transparency are achieved through looking "across" systems rather

than "inside" to expose power structures [18]. Although the limits of 'seeing' transparency might have been metaphorical so far, thinking about obfuscations pose practical urgent questions on how to imagine non-visual transparency. Our study reveals tensions with sight-centered ways of understanding transparency, equating transparency with sight assumes normative human ability and leaves out non-visual sensemaking. Similar to Bigham et al.'s phenomena of "not knowing what you don't know" in web accessibility [32], participants surfaced issues around not knowing if the obfuscation process occurred correctly.

Focusing on computer-generated descriptions for Blind people, MacLeod et al. suggests exploring the potential of adding confidence ratings to facilitate critical mistrust [91]. However, participants expressed that percentages do not seem to be useful in obfuscation. It is hard to assess what a certain percentage might mean. Additionally, AI systems might still misinterpret elements with high accuracy (e.g., facial recognition often misclassifies trans*/non-binary people while claiming a high confidence score [86, 111]). Contending with misrecognition, error and uncertainty is a core element of interacting with AI systems. However, mistakes made by obfuscation systems are typically only interpreted through sighted sensemaking, denying the agency of Blind and low vision people. The design of obfuscation systems, as we know it, actively conceals errors from Blind and low vision people. Future work ought to critically engage with accessible ways of communicating obfuscation outcomes to Blind and low vision people. Interdependence might be a useful way to think about non-visual transparency and safeguards.

Interdependence is a generative framework for thinking about trust and error in obfuscation because it moves away from eliminating system error towards establishing safeguards [23]. At its core, interdependence emphasizes negotiated relationships that are built on shared values like mutual trust [23, 28, 84]. While not necessarily communicating accuracy of obfuscation in the moment, safeguards ensure remediation when misrecognition happens. Focusing on navigation and VDS use, Abolrahmani et al. categorized various moments of errors, demonstrating that Blind people recognize that technology is not perfect, forgiving moments of errors in unfamiliar crowded environments while not forgiving severe cases like misidentifying restroom gender signs [6]. Through operationalizing interdependence, Bennett et al. expand reconciling with errors by arguing that "navigation systems will not be error free, so they instead direct research to support context-appropriate error and safety management" [23, pg. 10]. To safeguard incidents of error within obfuscation, participants noted opportunities to permanently delete data where obfuscation errors occurred. Our analysis reflects a need to move away from a focus on accuracy and obliterating error towards creating VDS-level protocols that such data would be handled with care through giving users options and control over their data. This an area for future work to further build upon by asking how might VDS companies notify users about errors and what types of controls do users want.

5.2 Design Directions

Here, we outline design directions and insights based on participants concerns with obfuscation, focusing on representation, distraction, and control. While some might be difficult to implement on a technical level, we believe there is value in imagining and working towards alternatives.

5.2.1 Working Towards Representational Obfuscation Datasets. As previously discussed, the privacy concerns of Blind and low vision people are dynamic, depending on a wide range of factors such as access needs and identity. Many participants worried that their own privacy considerations would not be represented in popular obfuscation datasets, leading to misrecognition. Further, datasets and models are often thought to be objective, precise, and temporally static [110]. This is antithetical to how privacy needs are fluid and prone to change given how they are intertwined with access. Thus,

a meaningful design direction would be towards working on representational, fluid, datasets that attend to cultural and dynamic access needs. Generally, data on disability is considered to be scarce, leading to creative data collection approaches such as online infrastructures for data gathering [105]. However, sharing details about what is constituted as private on online infrastructure might lead to harmful security-related implications. Researchers in the ORBIT (Object Recognition for Blind Image Training) project are exploring ways to collect data from a community-oriented lens, centering the needs of Blind and low vision people to personalize VDS [120]. Moving forward, one way to create and sustain representational and fluid obfuscation datasets is through brief, anonymous, periodic surveys or nudges sent to Blind and low vision communities to inquire about privacy concerns. With these insights, obfuscation datasets and models can be updated as necessary to include dynamic and cultural-specific privacy needs.

Before delving in this design direction, we invite researchers to grapple with the limits of inclusion and the potential harms of such framing [25, 74, 117]. It is important to note that Blind and low vision communities have long been engaging in the (often unpaid) labor of collecting datasets to repair accessibility failures of technology corporations. For example, operating from their own frustrations, Arab Blind and low vision VoiceOver users collectively document instances of misrecongition and error with Arabic screenreaders to share such resources with Apple. Researchers in academia and technology corporations need to recognize data collection as valuable labor and compensate accordingly. Working with sign language users, Bragg et al. have done extensive work on examining the ethical and privacy considerations of collecting data for sign language machine learning systems [37–39]. In a similar matter, we encourage obfuscation researchers to critically reflect and examine potential labor requests before beginning data collection. Additionally, as disclosing privacy concerns might be a stigmatizing experience, we encourage researchers to first establish rapport and trust with community members and provide adequate compensation for their time and expertise.

5.2.2 Minimizing the Labor of Obfuscation. The current trajectory of obfuscation systems assumes that boundaries between what should be obfuscated and what should not be is clear. Our findings complicate such linear views as evidenced by our participants' refusal of automatic obfuscation approaches. Even with content that might be universally thought to be private (e.g., pill bottles or bank information), participants wanted agency in obfuscation decision-making. Recent work in HCI argues for the importance of consent and dismissal within sociotechnical and AI systems [17, 77]. Obfuscation presents an interesting case to design for effective and simple mechanisms that do not add extra burdens on users. To achieve informed consent [77], Blind and low vision people must first be able to know the content targeted by obfuscation. Within our findings, the depth of description for such content varied. Some noted preference for full description of object (e.g., pill bottle) while others found general descriptors (e.g., private content) to be sufficient. Many raised concerns over obfuscation description leading to cognitive overload, especially as there is already labor involved in VDS without the addition of obfuscation. To resolve such issues, designers might consider introducing a menu option where users can have the agency to categorize obfuscation content as 'always allow', 'always hide' or 'ask every time' to potentially reduce efforts of repeated dismissal/consent and description processes. We emphasize that such content should be chosen by users and not pre-determined. Additionally, the depth of descriptions should be determined by users through options like 'full description' or vague indicators. As Danielle creatively suggests in section 4.3.1, there could an opportunity to enable users to customize specific alerts based on content of their choosing. Instead of spoken descriptions or indicators, these alerts will, hopefully, gently notify users of private content without adding much cognitive burden.

5.2.3 Allowing Granular Controls in Obfuscation. We learned from our participants that even within objects thought to be private (e.g., pill bottles), there still remains information that they need access to (e.g., medication dosage). Obfuscation algorithms ought to include granular control mechanisms that allow Blind and low vision people to obfuscate specific aspects of private content rather than the entire object. For instance, obfuscation algorithms could enable users to obfuscate specific regions (e.g., everything below document letterhead) or to obfuscate specific words and what follows (e.g., social security number). To further enable granular control over specific obfuscation regions, algorithms might also take a wide variety of inputs (e.g., words with a mix of letter and numbers or words that start with a specific letter). Popular blocklist approaches (i.e., which are trained to detect and obfuscate specific content such as faces) fail to capture the intricacies of an object that is thought to be private. For example, a financial document is not inherently private. Rather, the social security numbers or names included in such forms are often considered private and worthy of obfuscation. Allowing granular control in obfuscation gives users the agency to obfuscate and highlight specific elements of visual context, leading to potential improvement in visual description and greater sense of security. In a past study, Raval et al. introduced *privacy markers* as a way to provide users an opportunity to obfuscate an arbitrary area of their choosing in visual contexts [108]. While this approach addressed a wide variety of issues around such as system designer's failing to anticipate user privacy needs, their study focused on sighted participants. Moving forward, obfuscation and VDS researchers can gain inspiration from past work on non-visual image exploration [88] to allow for more granular level of controls in obfuscation. For example, Lee et al. developed a touch-based system for image exploration to expand computer generated captions such that Blind and low vision people can understand various aspects of visual content by double tapping into various regions of an image [88]. Researchers might take inspirations from image exploration approaches to enable users to obfuscate specific regions of visual content for certain, less complex, cases like using AI-based VDS for simple tasks at home. Given what has been establish in section 4.1.4, however, it could be difficult to adopt such approaches in tasks like navigation.

5.3 Study Limitations & Future Works

The goal of this work is to center the perspectives of Blind and low vision people on obfuscation technology. We focused on obfuscation specifically because it is considered to be the state-of-the-art approach to preserving privacy in visual contexts [15, 66, 73, 90] and past research calls for building and designing obfuscation systems to address privacy concerns in VDS [12, 66]. We inform such trajectory by contributing an interdependence lens towards obfuscating content. As it is outside the scope, our study does not include technological approaches beyond obfuscation and non-technological solutions (e.g., policy based) for addressing privacy concerns. Further, human-enabled VDS includes sighted volunteers and agents. Future work should consider their perspectives on obfuscation and how that might influence visual interpretation. Additionally, it is important to include bystanders in the design process of obfuscation technologies, attending to their privacy considerations.

Our methodological approach of semi-structured interviews embraces situated and local understandings instead of striving for generalizability and universality [70]. Semi-structured interviews allowed us to engage in creative conversations around the future of obfuscation without restricting participants' imaginations to particular affordances, benefits and limits of current obfuscation technologies. Other methods such as reoccurring design workshops, formative system deployments, or survey and participant observations could be valuable avenues to explore in future work to gain different depth of information on this topic.

Furthermore, since the original recruitment was among people who already use VDS, there is a self-selection bias towards those who continue to use VDS and does not capture those who refuse

to use VDS given privacy concerns. Understanding the perspectives of obfuscation from Blind and low vision with a wider range of perspectives, including those who do not use VDS, might provide richer insights. Additionally, one participant noted how their experience with ADHD shaped their potential interaction with obfuscation. Future work might consider recruiting those with multiple types of disabilities, in addition to visual disability, to understand these factors on obfuscation. Also, all interview participants live in the United States. As our findings included those with diverse racial and ethnic identities, we report how privacy practices are influenced by culture. However, it is also important to account for geographic locations beyond the U.S. because privacy is shaped by local laws, regulations and norms.

6 CONCLUSION

In response to emerging efforts to build obfuscation systems that address privacy concerns in VDS, our study explored the perspectives of Blind and low vision people on obfuscation. We found that the current trajectory of obfuscation research might fail to capture the needs of Blind and low vision people. Largely, participants refused automatic obfuscation approaches and wanted to meaningfully participate in shaping obfuscation. Our analysis illustrates several tensions with obfuscation, including non-visually confirming obfuscation outcomes and choosing obfuscation content. Through applying the framework of interdependence, we unpack and understand the frictions of obfuscation by 1) complicating privacy needs through considering its connection with access and identity 2) uncovering and paying attention to the labor Blind and low vision people already perform with VDS and 3) emphasizing the importance of safeguards when error occurs. We detail design directions that push the field of obfuscation forward.

ACKNOWLEDGMENTS

This material is based upon work supported by the National Science Foundation under Grants #1763297 and #1552503. We would like to express our gratitude to the participants in this study for their time and expertise, especially as the on-going COVID-19 pandemic made energy so scarce. The authors also appreciate and thank Rawan Alharbi, Maitham AL-Sunni, Ira Anjali Anwar, Cami Goray, Anhong Guo, John Rudnik, Harmanpreet Kaur, Nazanin Andalibi, Tawanna Dillahunt, Shwetha Rajaram, Saood AlMarzooqi, Stefany Cruz and our anonymous reviewers for their thoughtful feedback on earlier drafts of this work.

REFERENCES

[1] [n. d.]. https://www.bloomberg.com/news/videos/2021-08-18/the-apps-redefining-accessibility-video
[2] [n. d.]. Aira. https://aira.io/aira-live
[3] [n. d.]. Aira Privacy Policy. https://aira.io/privacy-policy
[4] [n. d.]. SeeingAI. https://www.microsoft.com/en-us/ai/seeing-ai
[5] 2019. The kindness of strangers: Volunteers use app to provide a helpful pair of eyes to those who are blind | CBC News. https://www.cbc.ca/news/canada/british-columbia/the-kindness-of-strangers-volunteers-use-app-to-provide-a-helpful-pair-of-eyes-to-those-who-are-blind-1.5201216
[6] Ali Abdolrahmani, William Easley, Michele Williams, Stacy Branham, and Amy Hurst. 2017. Embracing errors: Examining how context of use impacts blind individuals' acceptance of navigation aid errors. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. 4158–4169.
[7] Ali Abdolrahmani, Kevin M Storer, Antony Rishin Mukkath Roy, Ravi Kuber, and Stacy M Branham. 2020. Blind leading the sighted: drawing design insights from blind users towards more productivity-oriented voice interfaces. ACM Transactions on Accessible Computing (TACCESS) 12, 4 (2020), 1–35.
[8] Alessandro Acquisti, Ralph Gross, and Fred Stutzman. 2014. Face recognition and privacy in the age of augmented reality. Journal of Privacy and Confidentiality 6, 2 (2014).
[9] Dustin Adams, Lourdes Morales, and Sri Kurniawan. 2013. A qualitative study to support a blind photography mobile application. In Proceedings of the 6th International Conference on PErvasive Technologies Related to Assistive Environments. 1–8.

[10] Paarijaat Aditya, Rijurekha Sen, Peter Druschel, Seong Joon Oh, Rodrigo Benenson, Mario Fritz, Bernt Schiele, Bobby Bhattacharjee, and Tong Tong Wu. 2016. I-pic: A platform for privacy-compliant image capture. In Proceedings of the 14th annual international conference on mobile systems, applications, and services. 235–248.
[11] 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. 3523–3532.
[12] 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). 1929–1948.
[13] Kendra Albert, Emily Armbruster, Elizabeth Brundige, Elizabeth Denning, Kimberly Kim, Lorelei Lee, Lindsey Ruff, Korica Simon, and Yueyu Yang. 2020. Fosta in legal context. Colum. Hum. Rts. L. Rev. 52 (2020), 1084.
[14] Rawan Alharbi, Tammy Stump, Nilofar Vafaie, Angela Pfammatter, Bonnie Spring, and Nabil Alshurafa. 2018. I can't be myself: effects of wearable cameras on the capture of authentic behavior in the wild. Proceedings of the ACM on interactive, mobile, wearable and ubiquitous technologies 2, 3 (2018), 1–40.
[15] Rawan Alharbi, Mariam Tolba, Lucia C Petito, Josiah Hester, and Nabil Alshurafa. 2019. To mask or not to mask? balancing privacy with visual confirmation utility in activity-oriented wearable cameras. Proceedings of the ACM on interactive, mobile, wearable and ubiquitous technologies 3, 3 (2019), 1–29.
[16] Mahsa Alimardani and Mona Elswah. 2021. Digital Orientalism:# SaveSheikhJarrah and Arabic Content Moderation. Alimardani, Mahsa and Elswah, Mona. Digital Orientalism:# SaveSheikhJarrah and Arabic Content Moderation (August 5, 2021). In POMEPS Studies 43 (2021).
[17] Saleema Amershi, Dan Weld, Mihaela Vorvoreanu, Adam Fourney, Besmira Nushi, Penny Collisson, Jina Suh, Shamsi Iqbal, Paul N Bennett, Kori Inkpen, et al. 2019. Guidelines for human-AI interaction. In Proceedings of the 2019 chi conference on human factors in computing systems. 1–13.
[18] Mike Ananny and Kate Crawford. 2018. Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. new media & society 20, 3 (2018), 973–989.
[19] Payal Arora. 2019. Decolonizing privacy studies. Television & New Media 20, 4 (2019), 366–378.
[20] Ulla Autenrieth. 2018. Family photography in a networked age: Anti-sharenting as a reaction to risk assessment and behaviour adaption. (2018).
[21] Mauro Avila, Katrin Wolf, Anke Brock, and Niels Henze. 2016. Remote assistance for blind users in daily life: A survey about be my eyes. In Proceedings of the 9th ACM International Conference on PErvasive Technologies Related to Assistive Environments. 1–2.
[22] Andrew Begel, John Tang, Sean Andrist, Michael Barnett, Tony Carbary, Piali Choudhury, Edward Cutrell, Alberto Fung, Sasa Junuzovic, Daniel McDuff, et al. 2020. Lessons Learned in Designing AI for Autistic Adults. In The 22nd International ACM SIGACCESS Conference on Computers and Accessibility. 1–6.
[23] Cynthia L Bennett, Erin Brady, and Stacy M Branham. 2018. Interdependence as a frame for assistive technology research and design. In Proceedings of the 20th international acm sigaccess conference on computers and accessibility. 161–173.
[24] 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. 1–19.
[25] Cynthia L Bennett and Os Keyes. 2020. What is the point of fairness? Disability, AI and the complexity of justice. ACM SIGACCESS Accessibility and Computing 125 (2020), 1–1.
[26] Cynthia L Bennett, Burren Peil, and Daniela K Rosner. 2019. Biographical prototypes: Reimagining recognition and disability in design. In Proceedings of the 2019 on Designing Interactive Systems Conference. 35–47.
[27] Cynthia L Bennett and Daniela K Rosner. 2019. The Promise of Empathy: Design, Disability, and Knowing the" Other". In Proceedings of the 2019 CHI conference on human factors in computing systems. 1–13.
[28] Cynthia L Bennett, Daniela K Rosner, and Alex S Taylor. 2020. The care work of access. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. 1–15.
[29] Patricia Berne, Aurora Levins Morales, David Langstaff, and Sins Invalid. 2018. Ten principles of disability justice. WSQ: Women's Studies Quarterly 46, 1 (2018), 227–230.
[30] Jeffrey P Bigham and Patrick Carrington. 2018. Learning from the front: People with disabilities as early adopters of AI. Proceedings of the 2018 HCIC Human-Computer Interaction Consortium (2018).
[31] Jeffrey P Bigham, Chandrika Jayant, Hanjie Ji, Greg Little, Andrew Miller, Robert C Miller, Robin Miller, Aubrey Tatarowicz, Brandyn White, Samual White, et al. 2010. Vizwiz: nearly real-time answers to visual questions. In Proceedings of the 23nd annual ACM symposium on User interface software and technology. 333–342.
[32] Jeffrey P Bigham, Irene Lin, and Saiph Savage. 2017. The Effects of" Not Knowing What You Don't Know" on Web Accessibility for Blind Web Users. In Proceedings of the 19th international ACM SIGACCESS conference on

computers and accessibility. 101–109.
[33] Lindsay Blackwell, Jean Hardy, Tawfiq Ammari, Tiffany Veinot, Cliff Lampe, and Sarita Schoenebeck. 2016. LGBT parents and social media: Advocacy, privacy, and disclosure during shifting social movements. In Proceedings of the 2016 CHI conference on human factors in computing systems. 610–622.
[34] Mark Blythe. 2014. Research through design fiction: narrative in real and imaginary abstracts. In Proceedings of the SIGCHI conference on human factors in computing systems. 703–712.
[35] 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. 1055–1064.
[36] 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. 2117–2126.
[37] Danielle Bragg, Naomi Caselli, Julie A Hochgesang, Matt Huenerfauth, Leah Katz-Hernandez, Oscar Koller, Raja Kushalnagar, Christian Vogler, and Richard E Ladner. 2021. The FATE Landscape of Sign Language AI Datasets: An Interdisciplinary Perspective. ACM Transactions on Accessible Computing (TACCESS) 14, 2 (2021), 1–45.
[38] Danielle Bragg, Oscar Koller, Mary Bellard, Larwan Berke, Patrick Boudreault, Annelies Braffort, Naomi Caselli, Matt Huenerfauth, Hernisa Kacorri, Tessa Verhoef, et al. 2019. Sign language recognition, generation, and translation: An interdisciplinary perspective. In The 21st international ACM SIGACCESS conference on computers and accessibility. 16–31.
[39] Danielle Bragg, Oscar Koller, Naomi Caselli, and William Thies. 2020. Exploring Collection of Sign Language Datasets: Privacy, Participation, and Model Performance. In The 22nd International ACM SIGACCESS Conference on Computers and Accessibility. 1–14.
[40] 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. 260–269.
[41] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. Qualitative research in psychology 3, 2 (2006), 77–101.
[42] Virginia Braun and Victoria Clarke. 2019. Reflecting on reflexive thematic analysis. Qualitative Research in Sport, Exercise and Health 11, 4 (2019), 589–597.
[43] Virginia Braun and Victoria Clarke. 2021. Can I use TA? Should I use TA? Should I not use TA? Comparing reflexive thematic analysis and other pattern-based qualitative analytic approaches. Counselling and Psychotherapy Research 21, 1 (2021), 37–47.
[44] Robin N Brewer and Vaishnav Kameswaran. 2018. Understanding the power of control in autonomous vehicles for people with vision impairment. In Proceedings of the 20th International ACM SIGACCESS Conference on Computers and Accessibility. 185–197.
[45] Robin N Brewer and Vaishnav Kameswaran. 2019. Understanding trust, transportation, and accessibility through ridesharing. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. 1–11.
[46] Robin N Brewer and Anne Marie Piper. 2017. xPress: Rethinking design for aging and accessibility through an IVR blogging system. Proceedings of the ACM on Human-Computer Interaction 1, CSCW (2017), 1–17.
[47] Jed R Brubaker, Lynn S Dombrowski, Anita M Gilbert, Nafiri Kusumakaulika, and Gillian R Hayes. 2014. Stewarding a legacy: responsibilities and relationships in the management of post-mortem data. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. 4157–4166.
[48] Amy Bruckman. 2002. Studying the amateur artist: A perspective on disguising data collected in human subjects research on the Internet. Ethics and Information Technology 4, 3 (2002), 217–231.
[49] Finn Brunton and Helen Nissenbaum. 2015. Obfuscation: A user's guide for privacy and protest. Mit Press.
[50] Michele A Burton, Erin Brady, Robin Brewer, Callie Neylan, Jeffrey P Bigham, and Amy Hurst. 2012. Crowdsourcing subjective fashion advice using VizWiz: challenges and opportunities. In Proceedings of the 14th international ACM SIGACCESS conference on Computers and accessibility. 135–142.
[51] Kimberle Crenshaw. 1990. Mapping the margins: Intersectionality, identity politics, and violence against women of color. Stan. L. Rev. 43 (1990), 1241.
[52] Mary J Culnan and Pamela K Armstrong. 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. Organization science 10, 1 (1999), 104–115.
[53] Maitraye Das, Darren Gergle, and Anne Marie Piper. 2019. " It doesn't win you friends" Understanding Accessibility in Collaborative Writing for People with Vision Impairments. Proceedings of the ACM on Human-Computer Interaction 3, CSCW (2019), 1–26.
[54] Terrance de Vries, Ishan Misra, Changhan Wang, and Laurens van der Maaten. 2019. Does object recognition work for everyone?. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops.

52–59.
[55] Mariella Dimiccoli, Juan Marín, and Edison Thomaz. 2018. Mitigating bystander privacy concerns in egocentric activity recognition with deep learning and intentional image degradation. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 1, 4 (2018), 1–18.
[56] Paul Dourish. 2004. What we talk about when we talk about context. Personal and ubiquitous computing 8, 1 (2004), 19–30.
[57] Be My Eyes. [n. d.]. www.bemyeyes.com
[58] Chancey Fleet. 2021. Digital Frictions and Dark Patterns in Accessible Technology. https://www.youtube.com/watch?v=_eX5_iibP54
[59] Batya Friedman. 1996. Value-sensitive design. interactions 3, 6 (1996), 16–23.
[60] Rosemarie Garland-Thomson. 2001. Re-shaping, Re-thinking, Re-defining. Center for women policy studies (2001).
[61] Rosemarie Garland-Thomson. 2002. Integrating disability, transforming feminist theory. NWSA journal (2002), 1–32.
[62] Rosemarie Garland-Thomson. 2005. Feminist disability studies. Signs: Journal of women in Culture and Society 30, 2 (2005), 1557–1587.
[63] Erving Goffman. 1967. Interaction ritual: Essays on face-to-face interaction. (1967).
[64] Erving Goffman et al. 1978. The presentation of self in everyday life. Vol. 21. Harmondsworth London.
[65] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H Mhaidli, Kentaro Toyama, and Florian Schaub. 2018. Keeping a low profile? Technology, risk and privacy among undocumented immigrants. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. 1–15.
[66] 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/CVF Conference on Computer Vision and Pattern Recognition. 939–948.
[67] Danna Gurari, Yinan Zhao, Meng Zhang, and Nilavra Bhattacharya. 2020. Captioning images taken by people who are blind. In European Conference on Computer Vision. Springer, 417–434.
[68] Aimi Hamraie and Kelly Fritsch. 2019. Crip technoscience manifesto. Catalyst: Feminism, Theory, Technoscience 5, 1 (2019), 1–33.
[69] Vicki L Hanson, Anna Cavender, and Shari Trewin. 2015. Writing about accessibility. Interactions 22, 6 (2015), 62–65.
[70] Donna Haraway. 1988. Situated knowledges: The science question in feminism and the privilege of partial perspective. Feminist studies 14, 3 (1988), 575–599.
[71] Christina Harrington and Tawanna R Dillahunt. 2021. Eliciting Tech Futures Among Black Young Adults: A Case Study of Remote Speculative Co-Design. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. 1–15.
[72] Nancy Hartsock. 1983. The feminist standpoint: Developing the ground for a specifically feminist historical materialism. In Discovering reality. Springer, 283–310.
[73] Rakibul Hasan, Eman Hassan, Yifang Li, Kelly Caine, David J Crandall, Roberto Hoyle, and Apu Kapadia. 2018. Viewer experience of obscuring scene elements in photos to enhance privacy. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. 1–13.
[74] Anna Lauren Hoffmann. 2021. Terms of inclusion: Data, discourse, violence. New Media & Society 23, 12 (2021), 3539–3556.
[75] Megan Hofmann, Devva Kasnitz, Jennifer Mankoff, and Cynthia L Bennett. 2020. Living disability theory: Reflections on access, research, and design. In The 22nd International ACM SIGACCESS Conference on Computers and Accessibility. 1–13.
[76] Panagiotis Ilia, Iasonas Polakis, Elias Athanasopoulos, Federico Maggi, and Sotiris Ioannidis. 2015. Face/off: Preventing privacy leakage from photos in social networks. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. 781–792.
[77] Jane Im, Jill Dimond, Melody Berton, Una Lee, Katherine Mustelier, Mark S Ackerman, and Eric Gilbert. 2021. Yes: Affirmative Consent as a Theoretical Framework for Understanding and Imagining Social Platforms. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. 1–18.
[78] Sins Invalid. 2017. Skin, tooth, and bone–the basis of movement is our people: a disability justice primer.
[79] Alejandro Jaimes, Daniel Gatica-Perez, Nicu Sebe, and Thomas S Huang. 2007. Guest Editors' Introduction: Human-Centered Computing–Toward a Human Revolution. Computer 40, 5 (2007), 30–34.
[80] 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. 203–210.
[81] Rikke Bjerg Jensen, Lizzie Coles-Kemp, and Reem Talhouk. 2020. When the civic turn turns digital: Designing safe and secure refugee resettlement. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. 1–14.

[82] Hernisa Kacorri, Utkarsh Dwivedi, Sravya Amancherla, Mayanka Jha, and Riya Chanduka. 2020. IncluSet: A data surfacing repository for accessibility datasets. In The 22nd International ACM SIGACCESS Conference on Computers and Accessibility. 1–4.
[83] Hernisa Kacorri, Kris M Kitani, Jeffrey P Bigham, and Chieko Asakawa. 2017. People with visual impairment training personal object recognizers: Feasibility and challenges. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. 5839–5849.
[84] Alison Kafer. 2013. Feminist, queer, crip. Indiana University Press.
[85] Harmanpreet Kaur, Mitchell Gordon, Yiwei Yang, Jeffrey Bigham, Jaime Teevan, Ece Kamar, and Walter Lasecki. 2017. Crowdmask: Using crowds to preserve privacy in crowd-powered systems via progressive filtering. In Proceedings of the AAAI Conference on Human Computation and Crowdsourcing, Vol. 5.
[86] Os Keyes. 2018. The misgendering machines: Trans/HCI implications of automatic gender recognition. Proceedings of the ACM on human-computer interaction 2, CSCW (2018), 1–22.
[87] Katharina Krombholz, Adrian Dabrowski, Matthew Smith, and Edgar Weippl. 2017. Exploring design directions for wearable privacy. (2017).
[88] Jaewook Lee, Yi-Hao Peng, Jaylin Herskovitz, and Anhong Guo. 2021. Image Explorer: Multi-Layered Touch Exploration to Make Images Accessible. In The 23rd International ACM SIGACCESS Conference on Computers and Accessibility. 1–4.
[89] Ada Lerner, Helen Yuxun He, Anna Kawakami, Silvia Catherine Zeamer, and Roberto Hoyle. 2020. Privacy and activism in the transgender community. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. 1–13.
[90] Yifang Li, Nishant Vishwamitra, Bart P Knijnenburg, Hongxin Hu, and Kelly Caine. 2017. Effectiveness and users' experience of obfuscation as a privacy-enhancing technology for sharing photos. Proceedings of the ACM on Human-Computer Interaction 1, CSCW (2017), 1–24.
[91] 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. 5988–5999.
[92] Jennifer Mankoff, Gillian R Hayes, and Devva Kasnitz. 2010. Disability studies as a source of critical inquiry for the field of assistive technology. In Proceedings of the 12th international ACM SIGACCESS conference on Computers and accessibility. 3–10.
[93] Bill Marczak, Geoffrey Alexander, Sarah McKune, John Scott-Railton, and Ron Deibert. 2017. Champing at the cyberbit: Ethiopian dissidents targeted with new commercial spyware. (2017).
[94] Allison McDonald, Catherine Barwulor, Michelle L Mazurek, Florian Schaub, and Elissa M Redmiles. 2021. " It's stressful having all these phones": Investigating Sex Workers' Safety Goals, Risks, and Practices Online. In 30th {USENIX} Security Symposium ({USENIX} Security 21).
[95] Mia Mingus. 2017. Access Intimacy, Interdependence and Disability Justice. https://leavingevidence.wordpress.com/2017/04/12/access-intimacy-interdependence-and-disability-justice/
[96] Mia Mingus. 2017. Forced Intimacy: An Ableist Norm. https://leavingevidence.wordpress.com/2017/08/06/forced-intimacy-an-ableist-norm
[97] Sophie Morlin-Yron. 2017. The app lending eyes to the blind. https://www.cnn.com/2016/11/24/africa/be-specular-app-helps-the-blind/index.html
[98] Meredith Ringel Morris. 2020. AI and accessibility. Commun. ACM 63, 6 (2020), 35–37.
[99] Leo Neat, Ren Peng, Siyang Qin, and Roberto Manduchi. 2019. Scene text access: a comparison of mobile OCR modalities for blind users. In Proceedings of the 24th International Conference on Intelligent User Interfaces. 197–207.
[100] Denis Newman-Griffis, Jessica Sage Rauchberg, Rahaf Alharbi, Louise Hickman, and Harry Hochheiser. 2022. Alternative models: Critical examination of disability definitions in the development of artificial intelligence technologies. arXiv preprint arXiv:2206.08287 (2022).
[101] Ihudiya Finda Ogbonnaya-Ogburu, Angela DR Smith, Alexandra To, and Kentaro Toyama. 2020. Critical race theory for HCI. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. 1–16.
[102] Tribhuvanesh Orekondy, Mario Fritz, and Bernt Schiele. 2018. Connecting pixels to privacy and utility: Automatic redaction of private information in images. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 8466–8475.
[103] Kentrell Owens, Camille Cobb, and Lorrie Cranor. 2021. "You Gotta Watch What You Say": Surveillance of Communication with Incarcerated People. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. 1–18.
[104] Joon Sung Park, Michael S Bernstein, Robin N Brewer, Ece Kamar, and Meredith Ringel Morris. 2021. Understanding the Representation and Representativeness of Age in AI Data Sets. arXiv preprint arXiv:2103.09058 (2021).

[105] Joon Sung Park, Danielle Bragg, Ece Kamar, and Meredith Ringel Morris. 2021. Designing an Online Infrastructure for Collecting AI Data From People With Disabilities. In Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency. 52–63.
[106] Leah Lakshmi Piepzna-Samarasinha. 2018. Care work: Dreaming disability justice. arsenal pulp press Vancouver.
[107] Yolanda A Rankin and Jakita O Thomas. 2019. Straighten up and fly right: Rethinking intersectionality in HCI research. Interactions 26, 6 (2019), 64–68.
[108] Nisarg Raval, Animesh Srivastava, Ali Razeen, Kiron Lebeck, Ashwin Machanavajjhala, and Lanodn P Cox. 2016. What you mark is what apps see. In Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services. 249–261.
[109] Kat Roemmich and Nazanin Andalibi. 2021. Data Subjects' Conceptualizations of and Attitudes Toward Automatic Emotion Recognition-Enabled Wellbeing Interventions on Social Media. Proceedings of the ACM on Human-Computer Interaction 5, CSCW2 (2021), 1–34.
[110] Morgan Klaus Scheuerman, Alex Hanna, and Emily Denton. 2021. Do datasets have politics? disciplinary values in computer vision dataset development. Proceedings of the ACM on Human-Computer Interaction 5, CSCW2 (2021), 1–37.
[111] Morgan Klaus Scheuerman, Jacob M Paul, and Jed R Brubaker. 2019. How computers see gender: An evaluation of gender classification in commercial facial analysis services. Proceedings of the ACM on Human-Computer Interaction 3, CSCW (2019), 1–33.
[112] Ari Schlesinger, W Keith Edwards, and Rebecca E Grinter. 2017. Intersectional HCI: Engaging identity through gender, race, and class. In Proceedings of the 2017 CHI conference on human factors in computing systems. 5412–5427.
[113] Susan P Shapiro. 1987. The social control of impersonal trust. American journal of Sociology 93, 3 (1987), 623–658.
[114] Ashley Shew. 2020. Ableism, technoableism, and future AI. IEEE Technology and Society Magazine 39, 1 (2020), 40–85.
[115] Katta Spiel, Christopher Frauenberger, Os Keyes, and Geraldine Fitzpatrick. 2019. Agency of autistic children in technology research—A critical literature review. ACM Transactions on Computer-Human Interaction (TOCHI) 26, 6 (2019), 1–40.
[116] 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. 1–12.
[117] Nikki Stevens, Anna Lauren Hoffmann, and Sarah Florini. 2021. The unremarked optimum: whiteness, optimization, and control in the database revolution. Review of Communication 21, 2 (2021), 113–128.
[118] Kevin M Storer and Stacy M Branham. 2019. " That's the Way Sighted People Do It" What Blind Parents Can Teach Technology Designers About Co-Reading with Children. In Proceedings of the 2019 on Designing Interactive Systems Conference. 385–398.
[119] Cella M Sum, Rahaf Alharbi, Franchesca Spektor, Cynthia L Bennett, Christina N Harrington, Katta Spiel, and Rua Mae Williams. 2022. Dreaming Disability Justice in HCI. In CHI Conference on Human Factors in Computing Systems Extended Abstracts. 1–5.
[120] Lida Theodorou, Daniela Massiceti, Luisa Zintgraf, Simone Stumpf, Cecily Morrison, Edward Cutrell, Matthew Tobias Harris, and Katja Hofmann. 2021. Disability-first Dataset Creation: Lessons from Constructing a Dataset for Teachable Object Recognition with Blind and Low Vision Data Collectors. In The 23rd International ACM SIGACCESS Conference on Computers and Accessibility. 1–12.
[121] Anja Thieme, Cynthia L Bennett, Cecily Morrison, Edward Cutrell, and Alex S Taylor. 2018. " I can do everything but see!"–How People with Vision Impairments Negotiate their Abilities in Social Contexts. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. 1–14.
[122] Shari Trewin. 2018. AI fairness for people with disabilities: Point of view. arXiv preprint arXiv:1811.10670 (2018).
[123] Mika Vanhala, Kaisu Puumalainen, and Kirsimarja Blomqvist. 2011. Impersonal trust. Personnel Review (2011).
[124] Beatrice Vincenzi, Alex S Taylor, and Simone Stumpf. 2021. Interdependence in Action: People with Visual Impairments and their Guides Co-constituting Common Spaces. Proceedings of the ACM on Human-Computer Interaction 5, CSCW1 (2021), 1–33.
[125] Kandrea Wade, Jed R Brubaker, and Casey Fiesler. 2021. Protest Privacy Recommendations: An Analysis of Digital Surveillance Circumvention Advice During Black Lives Matter Protests. In Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems. 1–6.
[126] Glen W White, Jamie Lloyd Simpson, Chiaki Gonda, Craig Ravesloot, and Zach Coble. 2010. Moving from independence to interdependence: A conceptual model for better understanding community participation of centers for independent living consumers. Journal of Disability Policy Studies 20, 4 (2010), 233–240.
[127] Meredith Whittaker, Meryl Alper, Cynthia L Bennett, Sara Hendren, Liz Kaziunas, Mara Mills, Meredith Ringel Morris, Joy Rankin, Emily Rogers, Marcel Salas, et al. 2019. Disability, bias, and AI. AI Now Institute (2019).

[128] Rua M Williams and LouAnne E Boyd. 2019. Prefigurative politics and passionate witnessing. In The 21st International ACM SIGACCESS Conference on Computers and Accessibility. 262–266.

[129] Rua M Williams and Juan E Gilbert. 2019. Cyborg perspectives on computing research reform. In Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems. 1–11.

[130] Rua M Williams, Kathryn Ringland, Amelia Gibson, Mahender Mandala, Arne Maibaum, and Tiago Guerreiro. 2021. Articulations toward a crip HCI. Interactions 28, 3 (2021), 28–37.

[131] Richmond Y Wong, Deirdre K Mulligan, Ellen Van Wyk, James Pierce, and John Chuang. 2017. Eliciting values reflections by engaging privacy futures using design workbooks. Proceedings of the ACM on Human-Computer Interaction 1, CSCW (2017), 1–26.

[132] Richmond Y Wong, Ellen Van Wyk, and James Pierce. 2017. Real-fictional entanglements: Using science fiction and design fiction to interrogate sensing technologies. In Proceedings of the 2017 Conference on Designing Interactive Systems. 567–579.

[133] Shaomei Wu, Jeffrey Wieland, Omid Farivar, and Julie Schiller. 2017. Automatic alt-text: Computer-generated image descriptions for blind users on a social network service. In Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing. 1180–1192.

A INTERVIEW PROTOCOL

Note: This is a general guide for a semi-structured interview. During one-on-one meetings with participants, we were able to expand beyond the questions mentioned in the protocol and follow up on specific details shared by participants.

Hello! My name is Rahaf. I am a researcher at the University of Michigan, studying technology and disability. Thank you so much for taking the time out of your day to share your expertise with me! This interview will focus on visual description applications (such as Aira, SeeingAI, Be My Eyes, and many more). You will receive $35 at the end of the interview to thank you for your participation and expertise. At any point, please let me know if you need a break or if you want me to rephrase any question. Also, please feel free to skip any questions without explaining why you wish to do so. You can communicate that with just saying "skip" or "pass" and I will move on to the next question. As a reminder, you are the expert here and I really appreciate learning from you.

A.1 Current use and non-use of VDS

(1) Can you tell me about the steps you take when you want to get more information about your surroundings, scenery or any objects around you?
(2) Can you tell me about the visual description applications that you currently use?
   - Broadly, How do you describe these visual descriptions applications? What do they mean to you?
   - What do you usually request description for?
   - How do you use various types of visual description services differently? That is, when does it make sense to use [EXAMPLE VDS 1] over [EXAMPLE VDS 2]?
   - How do you think these applications are different from reaching out to family or friends to get visual descriptions?
   - There is no right or wrong answer here. I am curious What do you think happens after you submit an image to [example AI-enabled VDS] or end a video call with [example human-enabled VDS]? Where does that image or video go? How long do you think they should store the data for?
   - What are the benefits of keeping the data for X amount of time? What about the potential harms of storing for X time?
   - Who do you think should have access to it and what for?
(3) What are the aspects you like about using visual description applications? What are the aspects you dislike about using visual description applications?
(4) Can you tell me if there are any circumstances or situations where you did not feel comfortable using visual description services? How has that affected your use of these types of visual description technology?
(5) Can you recall anything that happened when using [EXAMPLE VDS that frequently use or other VDS application] that made you feel concerned or worried?
   - What happened?
   - Why do you think it happened? And why did it happen in [VDS application] particularly?
   - Did you do anything differently as a result?
   - What would have made you feel more comfortable?
(6) Broadly speaking, what are some challenges and considerations that you think blind people might experience when deciding whether they use these types of visual description technology?

A.2 Imagination Session

Thank you so much for sharing! Now, we're going to transition to thinking about new features or elements that do not exist in today's technology. So think of this as an activity where I will be asking you to imagine new and upcoming technologies. Let's say, hypothetically speaking, say [visual description service participant is familiar with] had a new update where they automatically hide things that are considered to be personal, embarrassing or sensitive by maybe putting a black box, blurring, or emoji on it so that visual description service providers wouldn't be able to tell exactly what is being concealed. Before moving on, do you have any questions about this scenario?

A.2.1 First impression, automation and data collection.

(1) Generally, what do you think about this type of 'hiding' technology?
(2) Thinking about how you use [EXAMPLE VDS] for [previously disclosed scenario], how do you think this hiding technology would change how use [EXAMPLE VDS]?
(3) Can you tell me about a time when you think using this hiding technology would have been helpful to you?
(4) When would you not feel comfortable using this technology?
(5) Broadly, what types of information or objects would you like to be kept private when using [preferred VDS]? What about from [less preferred VDS]?
(6) What could be some benefits of using this new technology or update? What could be some drawbacks when using this type of hiding technology?
(7) I know you mentioned a couple of negative aspects on using [EXAMPLE VDS]. Do you think this new hiding technology would exacerbate existing drawbacks? Why or why not?

A.2.2 Obfuscation Features.

(1) How would you imagine this new hiding technology would let you know if it has detected something worthy of hiding?
(2) What are the ways you imagine the [Example VDS] to communicate to you and other user that this 'hiding technology' is not working properly?
(3) After this hiding feature was applied, what kind of information would be helpful for you in understanding how much [EXAMPLE OBJECT INTERVIEWEE MENTIONED BEFORE] is concealed?
(4) Thinking back to how you usually use [EXAMPLE VDS], in your opinion, do you think that this new hiding technology is feasible?
(5) If there is one thing that you can tell the developers of this new technology, what would you say?

Received January 2022; revised April 2022; accepted May 2022