Privacy Concerns and Behaviors of People with Visual Impairments

Tousif Ahmed **Roberto Hoyle** **Kay Connelly** **David Crandall** **Apu Kapadia**
School of Informatics and Computing
Indiana University
Bloomington, IN, USA
{touahmed, rjhoyle, connelly, djcran, kapadia}@indiana.edu

ABSTRACT
Various technologies have been developed to help make the world more accessible to visually impaired people, and recent advances in low-cost wearable and mobile computing are likely to drive even more advances. However, the unique privacy and security needs of visually impaired people remain largely unaddressed. We conducted an exploratory user study with 14 visually impaired participants to understand the techniques they currently use for protecting privacy, their remaining privacy concerns, and how new technologies may be able to help. The interviews explored privacy not only in the physical world (e.g., bystanders overhearing private conversations) and the online world (e.g., determining if a URL is legitimate), but also in the interface between the two (e.g. bystanders 'shoulder-surfing' data from screens). The study revealed serious concerns that are not adequately solved by current technology, and suggested new directions for improving the privacy of this significant fraction of the population.

Author Keywords
Privacy; visually impaired people; wearable technology

ACM Classification Keywords
K.4.2 Computers and Society: Social Issues

INTRODUCTION
Visually impaired people face a variety of challenges in navigating a physical and social world that is often not designed with them in mind. Visual impairments include not only complete blindness, but also poor vision, such as the inability to read a newspaper with ordinary glasses.[1] In the United States alone, over 8 million people are visually impaired, and older people are especially affected — about 1 in 6 people over age 45 and 1 in 4 people over 75 years old [1].

One important challenge faced by visually impaired people is how to preserve their privacy and security in their daily lives. Sighted people are able to monitor their surroundings to protect themselves from privacy threats. For example, when using a mobile device in public, sighted people can obscure sight lines between the screen and nosy bystanders. When sharing a photo online (which, perhaps somewhat surprisingly, visually impaired people do as often as the average user [33]), sighted people can check that it does not include embarrassing or private content.

A wide variety of research has studied how technology can assist visually impaired people [7, 9, 26, 31, 34], often highlighting privacy concerns [16, 21, 27, 34]. Researchers have also studied security and privacy issues for visually impaired people in specific contexts such as Web authentication [17], CAPTCHAs [4,13,19,25], and smartphone authentication [3, 11]. However, the unique privacy and security needs of the visually impaired are not sufficiently understood from a broader scope. We seek to explore how emerging sensor and camera-enabled mobile technologies could eventually enhance privacy in not only electronic settings, but also physical settings (e.g., bystanders overhearing private conversations) and the interface between the two (e.g., bystanders 'shoulder-surfing' data from screens). Before trying to develop solutions, however, we need to understand how visually impaired people manage privacy using existing techniques and what their remaining privacy needs are. Understanding the specific privacy concerns and behaviors of visually impaired people, as well as their commentary on existing and anticipated technologies, will inform and guide technical solutions to assist these users in enhancing their privacy.

Specifically, we seek to answer three main research questions:

R1: *What are the privacy concerns of visually impaired people?* We seek to understand their physical privacy concerns both in public and private spaces, including in the context of using electronic devices. We also seek to understand their concerns about privacy in virtual interactions, such as in online social networking and media-sharing websites.

[1]Blindness is "central visual acuity of 20/200 or less in the better eye with corrective glasses or central visual acuity of more than 20/200 if there is a visual field defect in which the peripheral field is contracted to such an extent that the widest diameter of the visual field subtends an angular distance no greater than 20 degrees in the better eye." [1] A person with a visual impairment cannot "recognize a friend at arm's length even when wearing glasses or contact lenses, or cannot read ordinary newspaper print even when wearing glasses or contact lenses, or reports poor or very poor vision even when wearing glasses or contact lenses, or is blind in both eyes." [1]

CHI 2015, April 18–23, 2015, Seoul, Republic of Korea .

http://dx.doi.org/10.1145/2702123.2702334

R2: *How do visually impaired people manage their privacy?* We seek to understand the existing privacy practices and behaviors of visually impaired people, again in the context of physical spaces, computing devices, and virtual interactions. We also seek to understand any existing assistive technology they use to enhance their privacy.

R3: *Which new technologies could offer enhanced privacy for visually impaired users?* We seek to understand how mobile and wearable computing technologies could enhance the privacy of the visually impaired, by both soliciting feedback on researcher-generated ideas and by collecting original suggestions from visually impaired people.

To answer these questions, we conducted an exploratory user study through semi-structured in-person interviews with visually impaired people (N=14). We explored their privacy concerns, needs, and behaviors in three main settings: physical, online, and at the interface between the two (e.g. privacy leaks that occur when using technology in public). We found that participants were aware of and concerned about privacy and security, and face a variety of risks. One recurring theme in their responses was that being forced to depend on other people, especially strangers, was a major privacy risk. We found that participants used a variety of techniques and technologies to try to manage privacy, but they repeatedly expressed a desire for better solutions. Moreover, assistive technologies themselves often created additional privacy risks. For example, screen-reading technology allows visually impaired people to access the web through their phones, but bystanders may also be able to hear; wearing headphones solves that problem, but muffles the sense of hearing, further reducing their ability to sense their surroundings [3, 27].

We now describe our work in detail. After reviewing related work, we describe our study protocol and procedure, and then present our major findings. We then discuss implications on the design and development of privacy-enhancing devices.

RELATED WORK

There is a large body of work on understanding the accessibility needs of visually impaired people in general, and some of this has highlighted the privacy implications of accessible devices. In their study on mobile device adoption, Kane *et al.* [16] report that visually impaired people have privacy concerns about using mobile devices in screen-reading mode. Naftali *et al.* [21] and Ye *et al.* [34] also find that people with visual impairments are concerned about eavesdropping when using screen readers and voice-to-text in public.

The work of Azenkot *et al.* [3] was one of the first to study the security and privacy threats and concerns of visually impaired mobile device users. They report that most users in their study were not aware of mobile device security threats, and none had enabled passcode locks on their phones. Most participants were also not aware of the threats of eavesdropping or shoulder surfing. They introduce an accessible non-visual authentication system that is designed to resist eavesdropping. Our work builds on theirs by including visually impaired participants who are not blind, which their paper suggested as an important direction for future work; we find that these participants were much more aware of and concerned about the potential for eavesdropping. We also study possible solutions to eavesdropping beyond authentication scenarios as well as privacy issues beyond mobile devices.

Shinohara and Wobbrock [27] discuss how simply having or using assistive devices may invite privacy-invading questions (e.g., "how did you lose your sight?") or behaviors (e.g., trying to give unwanted help). Our participants did not report concerns about stigma, but we did not specifically direct our interviews towards social issues. More research on the social consequences of assistive technologies is needed, since their success may depend on overcoming these social barriers.

In the context of the web, Sauer *et al.* [25] identify the top security challenges of blind users, including inaccessible CAPTCHAs, spam, keyloggers, and so on. Our participants brought up several of these like inaccessible CAPTCHAs and spam, but also identified other challenges like trying to practice good password management with a visual impairment, and accessibility of online privacy settings. Other work has studied usable authentication techniques for the visually impaired. Haque *et al.* [11] propose authentication using smartphone accelerometer sensors, and Azenkot *et al.* [3] propose authentication by tapping the phone. Kuber *et al.* [17] propose a web-based authentication system for blind users to keep their passwords safe from shoulder surfers, while several researchers [4, 13, 19, 25] have proposed usable CAPTCHAs for the visually impaired. In this paper we more broadly study privacy-enhancing concerns, behaviors, and tools used throughout everyday life, in addition to online concerns.

Outside the privacy domain, several papers have studied using wearable computing devices to enhance accessibility for the visually impaired. Velazquez *et al.* [31] present a number of prototypes of assistive devices for blind people, such as a wearable tactile feedback device called BrailleWatch, and a mechatronic shoe insole that vibrates to give navigational directions. Shilkrot *et al.* [26] present a handheld device to support reading text, while other researchers [7,9,34] have designed navigational tools for the visually impaired. Inspired by this work on accessibility, we focus here on how these devices could improve the privacy of visually impaired users.

METHODS

We interviewed visually impaired participants to investigate our research questions. The interviews were semi-structured and in person, to not only explore reports of participants' concerns and behaviors, but also to witness them ourselves.

Interview Preparation and Process

Each interview was conducted by two researchers, one of whom interacted with the participant while the other took notes. The audio of the interviews was recorded and later transcribed. After approximately half of the interviews were complete, one of the researchers analyzed the transcripts using an iterative coding process with initial coding and identified concepts [22, 24]. The two researchers discussed the identified concepts and developed a category of concepts

based on our research questions. After each subsequent interview, they met to identify new concepts and added them to the list. This semi-structured interview design allowed us to pursue concepts identified from prior interviews and to adapt our questionnaire as needed. For example, several early participants reported concerns about medical records, so we added a question about this to our questionnaire.

We conducted separate interviews, with the exception of married participants who could choose to include their spouse in the interview, since spouses are mutually supportive and the presence of a spouse could improve recall of concerns and offer additional insight. We conducted interviews at places of participants' choosing, and provided transportation if needed.

Interview Protocol

We used the following categories of questions:

1. **Background.** We began by asking participants to characterize their degree and history of visual impairment, their current use of technology including assistive technologies, and the level of assistance that they require from others.
2. **Privacy concerns and behaviors.** We asked participants to describe their physical and virtual privacy concerns, and any privacy-enhancing behaviors they use. We also asked about specific topics, such as whether participants had any concerns about assistive devices, about people watching them, and about their comfort in requesting assistance.
3. **Novel ideas.** We introduced wearable devices, and gave a chance to try Google Glass. We then discussed our ideas for wearable assistive devices and asked whether they could help protect privacy. Finally, we asked if participants had anything to add, to identify unexplored areas.

Study Procedure

Recruitment and Enrollment

We recruited participants through Indiana University's disability services office, and through the Bloomington and Bedford (Indiana) chapters of the American Council of the Blind (ACB). They distributed our study ad to their members, and we recruited those who responded between July and September 2014. We also introduced our study at two ACB meetings.

Ethical Considerations

Our university human subjects ethics board approved our study. To obtain informed consent, we provided our information sheet via email so that participants could use accessibility tools. We also read the information sheet aloud if needed. Participants could skip any question, and we recorded interviews only after obtaining consent verbally or in writing.

Compensation

Each participant was compensated $15 at the end of the study.

FINDINGS

Participants

We interviewed 14 participants over a two month period. Table 1 summarizes their demographics, which included 5 men and 9 women, and a diverse range of ages from 18 to 70. Our participants included two married couples in which both partners were visually impaired, and three participants were married to sighted partners. The married couples chose to be interviewed jointly, while two of the three other married participants chose to have the sighted partners present. Two participants (P8 and P12) were both visually and hearing impaired. The interviews lasted between 25 and 100 minutes, with most about 45 minutes. Participants chose where to be interviewed, with most (N=7) choosing a public places, while others chose their home (N=5) or office (N=2).

Physical Privacy Concerns

We first discuss *concerns about physical privacy* (as opposed to those related to devices or the online world). We identified the following recurring themes: lack of independence, eavesdropping, embarrassment, and physical security concerns.

Lack of Independence

Visually-impaired people often need help from others, including strangers; they may need to ask bank employees to fill out financial documents, ask waiters to read the menu, or ask passersby to read street signs. These requests often involve revealing personal information to a stranger. In fact, most of the concerns that participants identified during our interviews seemed to result from this lack of independence, so we grouped them into the following subcategories.

Lack of accessibility. While many accessibility tools are available to access electronic documents, participants (N=9) expressed concerns about physical documents like letters and forms, especially ones with personal information. They reported receiving physical mail that they were unable to read on a daily basis. While some had devices that could scan and read content aloud, lack of standardization between documents frequently caused these tools to fail. Participants expressed concern about asking for assistance, since whether a document is sensitive is often not known *a priori*. P9 reported taking this risk because she did not have a choice:

> *I have to find out what a piece of paper says, so I have to ask someone to read it. It's a risk that you take.*

Filling out questionnaires and forms was another source of concern, for instance during visits to the doctor. P9 explained:

> *When you go to the doctor, there is a privacy issue. There are all these forms and they are never accessible, so somebody has to read them to you so you have to sign a document trusting that the person has read it correctly and completely to you.... Just because somebody takes you and gives you a ride to a doctor's office, they should not assume just because that person is a friend, that you want to share all of your health information with that friend.*

P3 expressed similar concerns about financial documents:

> *When I'm being asked to fill out paperwork at a bank, I can't do it so I have to ask the person to fill it out and have a verbal interview.*

Visually impaired people may need help reading restaurant checks or grocery bills. Cash transactions are particularly

ID	Age	Gender	Impairment	Device access method	Mobile device(s)	Assistive device(s)	Password management	Bank online?	Take photos?
P1	18-24	F	Low peripheral vision	Normal	iPhone	None	Save passwords	Yes	Yes
P2	18-24	F	Low vision, can see the shapes & outlines	Screen magnifier	iPhone, iPad	Magnifying glass	Memorize	Yes	Yes
P3	31-40	M	Low vision in one eye, blind in other	Screen magnifier, screen reader	iPhone	Ruby portable magnifier, portable reader	KeyChain	Yes	Yes
P4	31-40	F	Blind with light perception	Screen reader	iPhone	Braille displays, ebook players	Memorize, Braille	Yes	Yes
P5	31-40	M	Low vision, can see shapes	Screen reader	iPhone, iPad	iBook	Memorize	Yes	Yes
P6	41-50	M	Blind with light perception	Screen reader	iPhone	Victor Reader Stream	Store in text file	Yes	No
P7	41-50	F	Totally blind	Screen reader	iPhone	Victor Reader Stream, Ai Squared, Barcode Scanner	Change frequently	Yes	No
P8	51-60	M	Blind with light perception, hearing impaired	Screen reader, hearing aid	iPhone, landline	ZoomText, magnifier	Memorize	Yes	No
P9	51-60	F	Totally blind	Screen readers	iPhone	Braille embosser, color detector, electronic measuring tape, PenFriend, SignatureGuide, BrailleStylus, BrailleWatch, iPhone overlay	Braille	No	No
P10	51-60	M	Totally blind	Screen readers	Flip phone	DocuScan Plus Scanner	Memorize	Yes	No
P11	51-60	F	Totally blind	Screen readers	iPhone	DocuScan Plus Scanner, Prescription Reader	Braille	Yes	No
P12	51-60	F	Blind with light perception, hearing impaired	Screen readers, hearing aid	iPhone	OpenBook, Braille Printers, Braille Labels, Talking Timer	Save passwords, memorize	No	No
P13	61-70	F	Low vision, can see shapes	Screen readers	Landline	Barcode Reader, talking watch	Memorize	No	No
P14	61-70	F	Low vision in one eye, blind in other	Screen reader, magnifying tools	iPhone	CTC Scanner, Talking Calculator, Magnification Light	Memorize	Yes	Yes

Table 1. Summary of participant demographics and privacy behavior.

problematic since U.S. currency cannot be differentiated tactilely, so participants sometimes rely on others to identify bills. Although using debit or credit cards alleviates this problem, one participant mentioned that keypads on Point of Sale (POS) systems do not always have raised buttons, so she must ask strangers to enter her PIN — a potentially serious risk.

Finding items. It can be difficult for people with visual impairment to locate objects, and they often have to rely on others to find items in stores or even in their home. Requesting others' assistance in finding items can be uncomfortable, especially if the item is personal (e.g., a private medical item). P4 is learning to take photos for exactly this reason:

> *Once I learn to use the camera better I can take pictures of, like, boxes of unknown things that I have in my pantry that I don't know what they are anymore. It will read the barcode for me and tell me what it is and things like that.*

Navigation and transportation. Participants repeatedly raised challenges of navigation in the context of privacy, where the choice is sometimes asking a stranger for help and revealing private information, or maintaining privacy but risking physical harm. P12 struggles to find restrooms, especially in crowded places like airports. Others mentioned trying to navigate when routes change unexpectedly due to construction or maintenance. P3 once fell into an open manhole; he was using a cane, but by the time he had identified the hazard there was not enough time to avoid it. Assistive devices for navigation offer not only the prospect of improved privacy but also personal safety.

Eavesdropping

Eavesdropping was the next major category of privacy concerns indicated by participants (N=4), stemming from not knowing if other people are nearby. For instance, they mentioned concerns over giving out medical information in waiting rooms where others could be listening. P9 said:

> *I had gone to see a new doctor before, and they have to collect all of this private information from you about your health care and your lifestyles and everything. And, I actually had one of the attendants in the office; she came out to the waiting room, sat down and started filling out this paper. I said to her, 'I am assuming there is no one in the office but us right now.' Fortunately there wasn't, other than the person that had taken me to the office and that person was hard of hearing, so I let it go.*

Those who also have hearing problems felt even more exposed to eavesdropping, especially because they tend to speak loudly. P12 described her experience when donating blood:

> *They ask you some pretty private questions. It would be nice if there was a questionnaire that you can fill out independently, because they have to read it out to me. With me being hard of hearing they can't just whisper. That kind of bugged me. There's people on the other side of the little wall, that can probably hear everything that is going on.*

In these types of situations, participants reported either having to assume that there is nobody nearby, or asking a trusted person whether there is someone around.

Embarrassment

Some participants (N=3) reported embarrassing situations caused by not being able to sense the surroundings. P6 said:

> *One thing that bothers to me, and we encounter it so frequently. You can be standing there talking to somebody and one second you are talking to them and they answer you back. You keep on talking and they have since walked away. You were standing there jabbering, you don't know they have walked away. You look like fools.*

P4 mentioned a similar experience in her workplace:

> *There are a couple of people who work with us who are extremely shy people, so when I got on to them to at least*

say 'hi,' I was told that I was bullying them. I think I have no other way to know that they are in the room unless they say something. They don't have to talk to me, I just want to know that they are there.

Shinohara and and Wobbrock [27] reported on similar struggles of their participants trying to stay connected to others in the workplace, especially while using assistive devices.

Physical Security Concerns

We found that physical security and safety were major concerns for some participants (N=4), and these in turn created privacy concerns: maintaining one's home free from intrusion has long been considered a basic tenet of privacy [28]. For example, most participants were extremely cautious with home security, like hesitating to open the door when someone knocks unless they were expecting someone or recognized the person's voice. P13 said she felt scared when her husband is not home, even though they have a security system. People with both visual and hearing impairments were even more concerned; for instance, P8 expressed difficulty in hearing responses from people outside his door. P12 explained:

Security is a big thing with me, being totally blind, being hard of hearing. After my first husband passed away, we immediately got security systems in the house. I have an intercom outside, that's why I knew you were coming. That's why I had the door open. It's a scary world, when you have dual sensory loss like I do.

Some participants reported not feeling safe in public places. P13 and P14, who live with sighted spouses, specifically emphasized this concern. P13 expressed her feelings:

In public places, I get nervous if I am by myself, because I can't see very well. I don't usually go unless I am with someone. I don't like to be out by myself.

Computing Privacy Concerns

Like other populations, people with visual impairments use devices like smartphones, tablets, laptops, and personal computers. In fact, many participants said that these devices help them communicate and achieve greater independence. However, these devices also create privacy risks because of the vast amounts of personal data they store, and poor visual acuity makes it harder to safeguard this information. In this section we describe privacy concerns shared by participants about using computing devices. Many of these have been previously studied [3, 4, 13, 25, 34], and our study suggests they are still problems that have not yet been solved.

Eavesdropping

Participants were concerned about people eavesdropping on their digital devices, either visually or aurally.

Visual eavesdropping. Many of our participants (N=5) were aware of the threat of visual eavesdropping ('shoulder surfing') and tried not to use their devices in public. In this regard, our results differ from those of Azenkot *et al* [3], who found that their participants were largely unaware of these risks. One key difference however is that they studied only blind users, whereas we included visually impaired people who were not completely blind; the latter population is particularly susceptible because they often use large fonts. For example, P2 and P3, who are partially blind and use magnifying tools, were especially concerned about shoulder surfing. P2 is a student and feels uncomfortable using screen magnification in class, because anybody in the room can see what she is doing. P3 is particularly uncomfortable at work:

Because I use screen magnifiers, what I'm looking at on the screen is very large and it is very easy for other people to see and read it even if they are not intending to. I try to be mindful of that. No matter where my desk is placed, the screen is visible to somebody walking by. So, I don't have any privacy here. At home it is similar with the person I live with. I trust them to be considerate, but I'm sure they see things that I don't realize they see.

Aural eavesdropping. Many visually impaired people use accessibility features that read phone or computer screen content out loud. However, these features also create the risk of aural eavesdropping [3] of private information by bystanders, since visually impaired people may not be able to tell if bystanders are present. Generally, screen reader users are more concerned about aural eavesdropping, as has been reported in the literature [3, 21, 34]. We have found that those with both vision and hearing disabilities are more vulnerable to aural eavesdropping, as P8 explained:

I can't really see, so I depend on the audio. So, anybody in earshot can hear what my talking devices are saying. And because of my hearing aid I have to volume up a lot higher than most people would have. So, I have a concern of privacy there. I could use headphones but a lot of headphones are not compatible with hearing aids.

Security of Computing Devices

Strong passwords are key for computer security, but participants (N=5) reported struggling with password management because of their disability. Some recorded their passwords in a computer file and used screen readers to retrieve them, but this creates aural eavesdropping risks. Typing in passwords securely is also difficult; P3's screen reader makes a generic 'click' sound for each keypress when entering a password instead of the sound for the actual key, which prevents eavesdropping but makes it hard to enter the correct password. Only one participant used password manager software, while others said they were not very accessible and expressed skepticism about their security.

Some participants (N=2) expressed frustration with visual CAPTCHAs and other online mechanisms that try to prevent access to bots but also make websites much more difficult for the visually impaired to access. In P7's words:

CAPTCHA's are extremely annoying. We can't see what's on the screen and sometimes the audio is such that you can't even hear it.

Participants also felt that visual impairment left them more vulnerable to hacking. P6 shared:

My email account was hacked about a month ago twice within a two-week span. People started to get emails from

an account claiming to be me. I dumped my previous email provider and went to a different provider. It's very much of a privacy concern for us because unlike a lot of people, we don't always have the means to verify whether accounts or privacy information has been compromised.

Modern web browsers try to prevent some attacks like phishing schemes, but these features are not always accessible. For example, participants reported that screen readers interpret the URL in a browser by its display text rather than its contents, so it is difficult to identify a malignant URL. Other security cues like the lock icon verifying an encrypted connection are not easily confirmed by the visually impaired.

Technical Support

Like everyone, visually impaired people run into problems with their computing devices or need to learn how to use a new device, and require assistance either from technical support staff or from others. Some participants (N=5) reported concern about the privacy of the data on these devices, since it may be difficult for visually impaired people to verify that support staff are not accessing private information. P9 said:

When they were setting up my computer here and my laptop, I made sure that I had my work account separate than that of my personal account. The website person that helped me wanted to have remote access to my computer so that he could set up my account more quickly and I said no. I had a trainer before who had remote access to my computer and I wish I hadn't.

Assistive devices themselves sometimes break down or do not work properly. P9 also complained:

These software are not foolproof and that is the frustrating part. So, sometimes I have to go find someone sighted to read it for me, either from my screen or hard copies of something. It's really frustrating.

An additional complication is that the debugging information needed to diagnose a non-functional device is itself not accessible to a blind person. P9 noted that none of the accessibility tools installed on her computer worked until it was fully booted up, so she has no way to read errors during start-up.

Online Accessibility

Some participants (N=2) reported needing help accessing certain websites, creating privacy risks when private information is involved. P4 mentioned that a local bus operator's website is not accessible, so she gives her credit card number to someone else to buy tickets. P5's university website is not accessible, so he must ask someone to read his grades to him.

Privacy Concerns with Virtual Interaction

Like most users, visually impaired people share personal information online. Here we describe privacy concerns raised by our participants related to these virtual interactions.

Online Transactions

Many participants found online banking and shopping more accessible than visiting brick-and-mortar stores, but this was not a perfect solution because of concerns about the security of online transactions. These concerns mirror those of the broader population, especially among older adults (like many of our participants) [18]. P3's credit card information was recently stolen, making him more cautious and concerned about his online security. Others were sufficiently concerned about online security that they avoided it altogether. P12 said:

I am scared of online banking. I don't pay any kind of bills online, I don't even get bank statements online, everything is hard-copied.

Social Media Privacy

Like most users, visually impaired people use social networking platforms such as Facebook, Twitter, and LinkedIn. In fact, the visually impaired people Facebook status updates more frequently than average, while sharing and commenting on just as many photos [33], in part because these platforms help overcome challenges in interacting with others [6]. However, these sites involve sharing personal information and raise many privacy concerns for sighted and visually-impaired users alike [10]. Here we focus specifically on challenges created or heightened by visual impairments.

Most of our participants (N=11) reported using Facebook or other social-sharing websites, though most do not post much because of privacy concerns. One challenge they mentioned is the notoriously volatile and complicated nature of Facebook's privacy settings [8, 20]. Many participants (N=6) reported difficulty in adapting to new systems, so changes to user interfaces are problematic. P7 expressed her frustration:

Facebook is constantly changing, for us one minute we can use it and the next minute we can't because they are always changing the site. If I can get into the settings and find what I want like the advertising part, I try to stop all of that.

After posting content, it can be difficult for visually impaired users to confirm that the privacy settings are correct. P3 mentioned once trying to send a photo to specific friends and family but mistakenly made it public. He only realized this mistake when an unintended viewer commented on the photo.

Some applications help the visually impaired capture and manage photos [12, 15], but Adams *et al.* [2] report that blind users still face the risk of unintentionally sharing an embarrassing or sensitive image online. In our study, participants with low vision reported taking photos and magnifying them in order to see them. Only one completely blind participant (P4) takes photos. She was not concerned about sharing her photos because she avoids capturing any private images.

Privacy-Enhancing Behaviors

Participants used a variety of strategies to protect privacy.

Physical Privacy-Enhancing Behaviors

Most participants indicated that they address physical privacy concerns by requesting help from acquaintances. While some could depend on a sighted spouse to read their letters, for instance, others asked friends or acquaintances or relied on a scanner. Most participants mentioned that they were comfortable asking for help from a known person, including P2:

When it comes to reading out my credit card number, I have to ask friends who would not steal my stuff. I'd be pretty comfortable with that. It's about asking the right people.

Some participants hired assistants to deal with their personal matters, although it was difficult to trust them at first. When P4 first hired an assistant, she tested the assistant with a financial transaction by placing extra money in an envelope and checking whether it was returned.

Although some participants were skeptical about online banking, P10 and P11 believe that online services are a solution to financial privacy. P10 explained:

Before the computers were invented we had people read our checkbook, which was kind of privacy invasion. Now we don't have to, fortunately; because of modern technology now we can do all those things ourselves.

P11 added to her husband's argument:

Technology has come along and opened doors to blind people. Before, I used to hate to have someone fill out our checkbook, because you did not know if you could trust them. I felt that at that time you are taking a gamble, whereas now I can do it on my own and at least you now don't have to ask someone else.

To prevent physical eavesdropping, most participants tried to be alone. They generally did not engage in personal activities in public, and if they felt that someone could overhear their personal information, they looked for a more private space.

Many participants have home security systems, and several even demonstrated them to us. P14 explained:

I put in a security system since I cannot recognize who is at the door, in case my husband was not home. I would not open the door unless I know their voice or I know they are coming. I put that in for the sole reason that I am blind. If anybody opens a door, it automatically tells me. I can push a button and the police will automatically come.

Most participants used existing assistive technologies, including scanners or portable magnifiers to read documents. For labeling and finding items, they used bar-code scanners, PenFriends (which allows users to associate audio descriptions with a code on an adhesive label, and use a scanner to play back the description), color detectors, etc. For navigational help, most participants relied on canes or guide dogs. For money identification, they generally kept bills sorted and folded based on denomination, though some used smartphone applications. To identify items while shopping, some used smartphone apps like TapTapSee[2] to get an audio description of a photographed object (using a combination of computer vision and crowdsourcing).

Privacy-Enhancing Behaviors for Computing Devices

Participants reported several ways of preventing visual eavesdropping. Blind users reported using headphones to interact with their device, and either turned off their screens or used software to black it out (e.g., iOS Screen Curtain). In contrast, no partially impaired users used an auditory interface as a privacy-protecting mechanism, likely because the privacy benefits came at too high a cost (losing the visual channel).

To prevent aural eavesdropping, most participants used headphones, although this carries some risk: since visually impaired people rely on hearing in order to sense the environment, headphones leave them more vulnerable to other privacy and safety concerns (as Azenkot *et al* [3] also found). This caused many participants to avoid headphones, especially in situations involving social interactions. For example, during our interview with P9 in her office, she neither deactivated her screen-reader tool nor took other protective measures. Others simply reduced the speaker volume, and P8 and P9 felt screen readers play text so quickly that bystanders cannot understand what the screen reader tool is saying.

Most participants used caution with passwords. P2 memorizes long passwords, which she types rapidly to prevent anyone from seeing. P9 and P11 write their password in Braille. P6 stores his passwords in text files and changes them every three months. P12 stores some passwords in her browser's password management feature, but mostly types them manually. P3 discussed his struggle to find a good strategy:

I keep them either in Keychain in Mac OS X, or I also keep a list of passwords at home for personal things and [at the office] for work things. I keep that in a file on my computer. I have been trying to figure out what a good password utility to use is. I'm aware that keeping the list in the clear is not ideal. At home, my entire home folder is encrypted. When I'm logged in, it is unencrypted. If the computer was compromised, then the entire folder would be open.

Privacy-Enhancing Behaviors for Virtual Interactions

Of our participants' concerns about virtual interaction, online transactions, and especially online banking, were the most severe. P6 changes his passwords more frequently for these sites so that nobody can steal his information. P3 mentioned concern ever since his credit card information was stolen:

I'm mindful when I create a public wish list that it's public. I'm mindful of browser history and passwords that I used to log in. The transactions themselves, particularly after the card was compromised. I am aware and concerned.

While most (N=11) participants used online social networks, most were not very active, mainly sharing status updates, or others' photos or videos. P4 carefully checks privacy settings each time she shares on Facebook, while P3 is very selective about sharing any information. P12 echoed this strategy:

I am really cautious about what I post on there. I don't put anything like where I live, or if I'm going to be gone, for safety purposes.

When deciding whether to share a photo online, those who have low vision problems magnify the image to see what is in it. Others add metadata to photos, like time and place, to help identify them later. P4, who is completely blind and just getting started with photography, avoids taking private photos, and in fact uses Facebook to identify them later:

[2]TapTapSee: **http://taptapseeapp.com/**

Since I have only had my iPhone for a week, I have only taken three photos. I put those three photos on Facebook and just let everybody describe them, so that I could figure out which photo it was, based on what time I posted them.

New Technologies for Enhancing Privacy

Finally, our interviews explored technologies that could enhance the privacy and security of the visually impaired, with a focus on sensor-enabled mobile and wearable devices. After giving participants a chance to use Google Glass, we asked them for feedback on ideas that we had brainstormed ahead of time, and as well as for their own suggestions.

Feedback on our Ideas

In particular, we asked about seven specific features that a wearable camera-based device could implement.

1. Count the number of people nearby. Participants responded positively to this idea. P9 pointed out that knowing more about nearby people would be more helpful:

It would help you know how many people are around you when doing something private or a business interaction. However, how close are they? You'd have to know if they were within earshot or could see what you were doing.

2. Detect and identify specific faces nearby. Some participants were very excited about this idea, like P3:

When I'm walking by people I don't know who I'm walking by. If I think I know, I might say 'hi,' which may be embarrassing. So I typically don't, which is unfriendly. It would be nice to be able to recognize who is coming towards me like other people.

But P9 thought this would just create new privacy concerns:

If there's something that can identify people we have given up a lot of privacy. Not only can I identify people but someone can identify me. I would not want something that could identify someone automatically.

3. Identify the room a user is currently in. This idea received mixed reviews. Some participants responded that they can already tell based on sound, while others liked this idea.

4. Assist with navigation. Most participants reported that any application that could aid them in navigation would be helpful. Some mentioned that the map applications on their smartphones are not very accessible. P5 explained:

In some areas, I want to know where Starbucks is. I'm looking for a GPS for blind people, to tell me how we can, by walking, go to a certain place. I use Google Maps sometimes. I try to memorize the directions and go to that place.

5. Detect security cameras nearby. We thought visually impaired people might want a device to detect cameras, since sighted people can notice them and modify their behavior accordingly. P4 disliked this idea, saying that knowing about security cameras would make her feel paranoid. P6 and P7 liked it, saying that they want to be aware of anything that a sighted person is [27]. Other participants did not dislike the idea but felt it was not necessary, like P9:

I don't think about that since we are all living with cameras and I'm not out committing crimes.

6. Prevent shoulder surfing. Participants were very receptive to ideas to prevent shoulder surfing. Some low vision participants suggested that Google Glass could magnify whatever they are looking at, which could prevent visual eavesdropping since the Glass display is more private than most devices [23] (though determined attackers could likely spy on the transparent display (in reverse) with a telephoto lens).

7. Organize photo albums. Most participants liked the idea of an automated tool to analyze and describe photos for them, whether they personally take the photos or not. P3 explained:

I have a lot of photos, I like taking them. More and more these days I look at photos and can't figure out what I'm looking at. It depends on the contrast, lighting, angles.

Participant Ideas

We also solicited ideas from participants on using wearable devices to enhance privacy. Two ideas came up repeatedly in early interviews, so we incorporated them in later interviews. The first was to help find items using wearable devices; many participants said that existing locators were complex and expensive. P4 often drops belongings in laundry, so would like a device to help find items there. Others suggested barcode scanning on wearable devices to find items in stores. They also gave positive feedback about wearable devices that could read documents, as opposed to existing devices that are not as portable or convenient.

Another idea was a system to detect hazards and obstacles, like open manholes or warning signs. OrCam[3] identifies pedestrian signals at intersections, but participants felt that a more general version to identify other signs would be helpful.

DISCUSSION AND IMPLICATIONS

Our interviews made it clear that participants struggle with various types of security and privacy risks on a daily basis. Some of these are similar to the risks all people face but are heightened by visual impairments, whereas others are unique to the visually impaired. Participants expressed needs for better tools to protect privacy and security, and most were excited about the potential of mobile and wearable technology.

Assistive devices. Of course, a variety of assistive devices are already available to help the visually impaired. However, participants felt that many of them are too expensive, do not work well, or are not user friendly. P5, for example, felt learning to use an existing device is too time consuming, and found it easier and more cost-effective to hire an assistant. Wearable devices like Google Glass may help reduce cost and complexity, similar to how smartphones running user-installed apps have replaced multiple, dedicated devices such as audio recorders, GPS receivers, and cameras, providing a single integrated platform with lower cost and greater convenience.

Monitoring surroundings. A recurring theme throughout our interviews was the need to monitor surroundings, e.g., to know whether people are within earshot, to detect obstacles

[3] OrCam. `http://www.orcam.com/`

or hazards while walking, to locate and identify objects, and so on. These functions could be implemented as smartphone apps, but would require visually impaired users to take pictures manually, and only 5 of our 14 participants reported that they are able to take pictures. Head- or body-mounted cameras could be a viable alternative. Wearable cameras also could be 'always-on,' continuously analyzing the video feed and alerting the user whenever something unusual or suspicious is detected [29].

A key technical challenge would be how to recognize scene content. Unfortunately, while computer vision is progressing rapidly, state-of-the-art technology cannot perform these tasks accurately in unconstrained environments. One possibility is to use a combination of computer vision and crowdsourcing, which TapTapSee (reportedly) and Vizwiz [5] use to implement object detection on smartphones. For instance, computer vision could be used to detect potential hazards on a sidewalk, but then the relevant video frames could be sent to a sighted person (e.g., a friend or Mechanical Turk user) for verification. Of course, involving real people introduces the additional privacy challenges of allowing other people to see a person's wearable camera feed. This suggests that more work is needed on how to detect private content in images automatically, a problem that has recently been studied in the context of camera-based lifelogging [14, 30].

Another way of sidestepping the difficult computer vision problem is to incorporate data from non-visual sensors. For instance, instead of counting or identifying people using computer vision, one could exploit the fact that many people carry smartphones, so that Bluetooth signals could be used to estimate how many people are nearby as well as to identify certain people uniquely. GPS receivers and nascent indoor localization technology (like Apple's iBeacon) can be used to geo-locate users; systems could crowd-source reports of sidewalk hazards like construction zones and push notifications to visually impaired people who are nearby.

Feedback. Of course, an effective device would have to communicate information efficiently to the user, and a system that provides too many notifications could overwhelm and annoy the user. One solution would be to allow the user to provide privacy policies that could be executed automatically, depending on context. For example, a policy could turn off the screen and stop announcing emails if a bystander is nearby. Another policy could suppress all notifications in the home, except for emergencies like when an intruder is detected.

Limitations. Finally, we would like to acknowledge the limitations of our study and the opportunities for future work. Our participant sample was small, limited to one geographic area (southern Indiana), and restricted to those who chose to respond to an ad about privacy, so it is difficult to know how well our findings generalize to the greater population. Our participants were also older than average, and it is well-known that privacy concerns differ with age [18] (although the visually-impaired population itself is biased towards older adults, since 82% of the blind are over age 50 [32]). Studying privacy needs of younger populations (like teens and college students) would be interesting future work. In addition, our proposed solution space was biased towards wearable technologies, since we believe these may provide a hands-free, easy-to-use solution, although our participants did give their own feedback and alternative suggestions.

CONCLUSION

To better understand the privacy concerns and needs of visually impaired people, we conducted interviews with 14 visually impaired people. Our findings show that while the privacy concerns of people with visual impairments overlap with sighted people, there are also significant differences, due in part to their disability but also because of systems that were not designed with them in mind. Our participants were particularly aware of and concerned about these risks, and shared a variety of coping mechanisms to deal with them. They were generally excited about the potential for new wearable and mobile technologies to improve their privacy and independence. We hope that this research leads towards the implementation of some of these tools, which could have a major impact on the well-being of this underserved population.

ACKNOWLEDGMENTS

This material is based upon work supported in part by the National Science Foundation under grants CNS-1408730, CNS-1016603, CNS-1252697, and IIS-1253549, and by a Google Research Award. We thank Prerna Rustagi for helping us develop the initial Interview Protocol. We especially thank our participants, as well as Barbara Salisbury and Rita Kersh from the Bloomington and Bedford chapters of the American Council for the Blind, and Dorothy Lenard from IU Disability Services for Students, for helping us recruit participants.

REFERENCES

1. The lighthouse national survey on vision loss: The experience, attitudes and knowledge of middle-aged and older Americans. Tech. rep., The Lighthouse Inc, 1995.
2. Adams, D., Morales, L., and Kurniawan, S. A qualitative study to support a blind photography mobile application. In *International Conference on Pervasive Technologies Related to Assistive Environments* (2013), 1–8.
3. Azenkot, S., Rector, K., Ladner, R., and Wobbrock, J. Passchords: Secure multi-touch authentication for blind people. In *International ACM SIGACCESS Conference on Computers and Accessibility* (2012), 159–166.
4. Bigham, J. P., and Cavender, A. C. Evaluating existing audio CAPTCHAs and an interface optimized for non-visual use. In *SIGCHI Conference on Human Factors in Computing Systems* (2009), 1829–1838.
5. Bigham, J. P., Jayant, C., Ji, H., Little, G., Miller, A., Miller, R. C., Miller, R., Tatarowicz, A., White, B., White, S., and Yeh, T. Vizwiz: Nearly real-time answers to visual questions. In *ACM Symposium on User Interface Software and Technology* (2010), 333–342.
6. Brady, E., Morris, M. R., Zhong, Y., White, S., and Bigham, J. P. Visual challenges in the everyday lives of blind people. In *SIGCHI Conference on Human Factors in Computing Systems* (2013), 2117–2126.

7. Dakopoulos, D., and Bourbakis, N. Wearable obstacle avoidance electronic travel aids for blind: A survey. *IEEE Transactions on Systems, Man, and Cybernetics 40*, 1 (2010), 25–35.
8. Debatin, B., Lovejoy, J. P., Horn, A.-K., and Hughes, B. N. Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication 15* (2009), 83–108.
9. Fiannaca, A., Apostolopoulous, I., and Folmer, E. Headlock: A wearable navigation aid that helps blind cane users traverse large open spaces. In *Proceedings of the 16th International ACM SIGACCESS Conference on Computers & Accessibility* (2014), 19–26.
10. Gross, R., and Acquisti, A. Information revelation and privacy in online social networks. In *ACM Workshop on Privacy in the Electronic Society* (2005), 71–80.
11. Haque, M., Zawoad, S., and Hasan, R. Secure techniques and methods for authenticating visually impaired mobile phone users. In *IEEE International Conference on Technologies for Homeland Security* (2013), 735–740.
12. Harada, S., Sato, D., Adams, D. W., Kurniawan, S., Takagi, H., and Asakawa, C. Accessible photo album: Enhancing the photo sharing experience for people with visual impairment. In *SIGCHI Conference on Human Factors in Computing Systems* (2013), 2127–2136.
13. Holman, J., Lazar, J., Feng, J. H., and D'Arcy, J. Developing usable CAPTCHAs for blind users. In *International ACM SIGACCESS Conference on Computers and Accessibility* (2007), 245–246.
14. Hoyle, R., Templeman, R., Armes, S., Anthony, D., Crandall, D., and Kapadia, A. Privacy behaviors of lifeloggers using wearable cameras. In *ACM International Joint Conference on Pervasive and Ubiquitous Computing* (2014), 571–582.
15. Jayant, C., Ji, H., White, S., and Bigham, J. P. Supporting blind photography. In *International ACM SIGACCESS Conference on Computers and Accessibility* (2011), 203–210.
16. Kane, S. K., Jayant, C., Wobbrock, J. O., and Ladner, R. E. Freedom to roam: A study of mobile device adoption and accessibility for people with visual and motor disabilities. In *International ACM SIGACCESS Conference on Computers and Accessibility* (2009).
17. Kuber, R., and Sharma, S. Toward tactile authentication for blind users. In *International ACM SIGACCESS Conference on Computers and Accessibility* (2010).
18. Kwasny, M., Caine, K., Rogers, W., and Fisk, A. Privacy and technology: folk definitions and perspectives. In *CHI Extended Abstracts on Human Factors in Computing Systems* (2008).
19. Lazar, J., Feng, J., Brooks, T., Melamed, G., Wentz, B., Holman, J., Olalere, A., and Ekedebe, N. The SoundsRight CAPTCHA: An improved approach to audio human interaction proofs for blind users. In *SIGCHI Conference on Human Factors in Computing Systems* (2012), 2267–2276.
20. Liu, Y., Gummadi, K. P., Krishnamurthy, B., and Mislove, A. Analyzing Facebook privacy settings: User expectations vs. reality. In *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference* (2011), 61–70.
21. Naftali, M., and Findlater, L. Accessibility in context: Understanding the truly mobile experience of smartphone users with motor impairments. In *International ACM SIGACCESS Conference on Computers & Accessibility* (2014), 209–216.
22. Renner, M., and Taylor-Powell, E. Analyzing qualitative data. Tech. rep., University of Wisconsin, 2003.
23. Roesner, F., Kohno, T., and Molnar, D. Security and privacy for augmented reality systems. *Communications of the ACM 57*, 4 (Apr. 2014), 88–96.
24. Saldana, J. *The Coding Manual for Qualitative Researchers*. Sage, Los Angeles, California, 2009.
25. Sauer, G., Holman, J., Lazar, J., Hochheiser, H., and Feng, J. Accessible privacy and security: a universally usable human-interaction proof tool. *Universal Access in the Information Society 9*, 3 (2010), 239–248.
26. Shilkrot, R., Huber, J., Liu, C., Maes, P., and Nanayakkara, S. C. A wearable text-reading device for the visually-impaired. In *CHI Extended Abstracts on Human Factors in Computing Systems* (2014), 193–194.
27. Shinohara, K., and Wobbrock, J. O. In the shadow of misperception: Assistive technology use and social interactions. In *SIGCHI Conference on Human Factors in Computing Systems* (2011), 705–714.
28. Solove, D. J. A taxonomy of privacy. *University of Pennsylvania Law Review 154*, 3 (Jan. 2006), 477–566.
29. Templeman, R., Hoyle, R., Kapadia, A., and Crandall, D. Reactive security: Responding to visual stimuli from wearable cameras. In *Workshop on Usable Privacy & Security for Wearable and Domestic Ubiquitous Devices* (2014), 1297–1306.
30. Templeman, R., Korayem, M., Crandall, D., and Kapadia, A. PlaceAvoider: Steering first-person cameras away from sensitive spaces. In *Annual Network and Distributed System Security Symposium* (2014).
31. Velázquez, R. Wearable assistive devices for the blind. In *Wearable and Autonomous Biomedical Devices and Systems for Smart Environment* (2010), 331–349.
32. Visual Impairment and Blindness, World Health Organization fact sheet 282, 2014.
33. Wu, S., and Adamic, L. A. Visually impaired users on an online social network. In *SIGCHI Conference on Human Factors in Computing Systems* (2014), 3133–3142.
34. Ye, H., Malu, M., Oh, U., and Findlater, L. Current and future mobile and wearable device use by people with visual impairments. In *SIGCHI Conference on Human Factors in Computing Systems* (2014), 3123–3132.