Understanding the Physical Safety, Security, and Privacy Concerns of People with Visual Impairments

With the help of various assistive devices, people with visual impairments can live their lives with greater independence both online and offline. Yet significant work remains to understand and address their safety, security, and privacy concerns, especially in the physical, offline world. The authors investigate the physical safety, security, and privacy concerns of people with visual impairments through two sets of interviews, and find out how they manage these concerns and how assistive technologies could help. The research also proposes design considerations for camera-based devices that would help people with visual impairments monitor for potential threats around them.

Tousif Ahmed
Indiana University Bloomington

Roberto Hoyle
Oberlin College

Patrick Shaffer,
Kay Connelly,
David Crandall, and
Apu Kapadia
Indiana University Bloomington

Visual impairments range from total blindness to a significant degradation of sight that can't be corrected with corrective lenses or surgery.[1] People with these impairments face a variety of challenges in their daily lives, ranging from performing everyday household activities to navigating the physical world. Technology has helped overcome many of these challenges, for example, talking microwave ovens and vacuum cleaners have made household appliances more accessible, while smartphone mapping software and document readers help people navigate and sense the visual world around them.[2]

Even though these devices make it easier to perform various daily tasks, they don't directly address people's physical safety, security, and privacy needs. For instance, current technologies don't help monitor the surroundings to check for suspicious people who might be trying to steal cash or to overhear private conversations. Although researchers have begun to highlight physical privacy and security risks in the context of computer use for people with visual impairments — for example, Shiri Azenkot and colleagues discuss shoulder surfing of mobile devices,[3] and Shaun K. Kane and colleagues discuss discomfort

 Published by the IEEE Computer Society

with screen readers and magnifiers due to privacy concerns[4] — more remains to be understood about physical risks beyond electronic devices.

Through two sets of interviews of people with visual impairments we identify their physical safety, security, and privacy issues, finding out how they manage these concerns and how assistive technologies could help alleviate them. In this article, we summarize the results of our study. Then, we discuss our envisioned camera-based solution, including design considerations that should be addressed in these devices.

Participants

We conducted two separate sets of in-person, semistructured interviews (reported in conference papers[5,6]) of 33 individuals with visual impairments to shed light on concerns and coping strategies related to their physical privacy (for example, bystanders overhearing private conversations), security (for example, intruders invading personal spaces), and safety (for example, thieves assaulting them on the street). In both studies, we explicitly asked our participants about their concerns, their coping behaviors, and their suggestions for technological, camera-based solutions to address their concerns. To uncover issues unique to specific environments, we conducted the two sets of interviews in contrasting places in the US: a suburban college town (Bloomington, Indiana, with 14 participants)[5] and a large metropolitan area (San Francisco, California, with 19 participants).[6] We found some differences between these groups: urban participants focused much more on physical safety and security, for example, while the suburban population focused more on privacy.

Our long-term goal is to design and develop assistive solutions that better address physical privacy, security, and safety. Camera-based devices have shown promise in addressing the accessibility needs of people with visual impairments,[7,8] so our interviews discussed camera-based solutions to provide privacy, security, and safety information. In our interviews, we briefly introduced participants to wearable cameras by demonstrating Google Glass. We then elicited high-level design considerations that would help define the requirements for an eventual real device. For example, participants reported that discreetness is important, which will inform actual device design requirements such as size, location on the body, and modality of interaction.

Our participant pool was diverse, including a variety of age groups (median age 41 to 50), occupations (for example, student, technology instructor, organization coordinator, and programmer), and types and degree of visual impairment from complete blindness (12 participants), to being able to distinguish between light and dark (9 participants), to being able to see shapes and read with magnification (12 participants). Table 1 summarizes the demographic information.

The interviews were audio-recorded. We analyzed the transcribed interviews to inductively develop a set of codes. Two researchers coded excerpts of the transcripts and the authors iterated on the coding scheme until it achieved a satisfactory level of interrater reliability (Cohen's $\kappa = 0.79$). In both studies, we had codes in three main categories: concerns, defensive behavior, and technology requirements.

Concerns

Our participants expressed a variety of concerns related to physical privacy as well as physical security and safety, due to not being able to fully perceive their surroundings.

The most common privacy concern, mentioned by a majority of our participants, was other people eavesdropping on conversations, or shoulder-surfing to see private information (for example, from a smartphone or personal document). This concern, primarily caused by a hampered ability to sense if people are in the vicinity, was frequently mentioned in the context of situations when participants have to share personal information with others. For example, many participants reported discomfort in sharing health information with staff in a doctor's office waiting room because they didn't know whether other people could overhear their conversation. For example, one participant explained:

> 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. … One of the attendants in the office 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.

Participants reported similar concerns while filling out forms at the bank, sharing personal

ID	Gender	Age group	Impairment type	Technology usage
P1	F	18–24	Low peripheral vision	iPhone
P2	F	18–24	Low vision, can see shapes and outlines	iPhone, iPad
P3	F	18–24	Low vision	iPhone, laptop
P4	M	18–24	Low vision	iPhone, laptop
P5	F	25–30	Totally blind	iPhone
P6	F	25–30	Blind in one eye, light perception in other	iPhone, laptop
P7	M	25–30	Low vision	iPhone, laptop
P8	F	31–35	Totally blind	Windows phone, regular and Braille laptop
P9	F	31–35	Totally blind	iPhone, portable Braille computer
P10	M	31–35	Low vision in one eye, blind in other	iPhone, Ruby portable magnifier, portable reader
P11	F	31–35	Blind with light perception	iPhone, Braille displays, ebook players
P12	M	31–35	Low vision, can see shapes	iPhone, iPad, iBook
P13	M	31–35	Totally blind	iPhone, iPad, MacBook
P14	F	31–35	Totally blind	Android smartphone, tablet, laptop
P15	M	31–35	Low vision	iPhone, laptop
P16	F	36–40	Blind with light perception	iPhone, laptop
P17	F	41–50	Totally blind	Android
P18	M	41–50	Blind with light perception	iPhone, Victor Reader Stream
P19	F	41–50	Totally blind	iPhone, Victor Reader Stream, WindowEyes, barcode scanner
P20	M	41–50	Blind in one eye, low vision in other	Android smartphone, laptop
P21	M	41–50	Blind with light perception, can see shapes	Android smartphone, laptop
P22	M	51–60	Blind with light perception, hearing impaired	iPhone, ZoomText magnifier
P23	F	51–60	Totally blind	iPhone, Braille embosser, PenFriend, signature guide, Braille stylus, Braille watch
P24	M	51–60	Totally blind	Flip phone, DocuScan Plus scanner
P25	F	51–60	Totally blind	iPhone, DocuScan Plus scanner, prescription reader
P26	F	51–60	Blind with light perception, hearing impaired	iPhone, OpenBook, Braille printers
P27	M	51–60	Low vision	Smartphone, laptop
P28	M	51–60	Totally blind	iPhone
P29	F	61–70	Blind with light perception, can see shapes	Cellphone, laptop
P30	F	61–70	Totally blind	iPhone
P31	M	61–70	Low vision	Landline phone, iPad, laptop
P32	F	61–70	Low vision, can see shapes	Barcode reader, talking watch
P33	F	61–70	Low vision in one eye, blind in other	iPhone, scanner, talking calculator, magnification light

Table 1. Demographic information for our study participants.

information in their office, having personal conversations on the phone in public, or entering their PIN at an ATM or store checkout.

Ironically, assistive devices themselves actually create privacy concerns. People with visual impairments typically use screen readers or magnifiers to access information on their smartphones, for example. Most participants said these technologies makes it easier for bystanders to see or hear private information, and sometimes strategies for countering these potential privacy leaks themselves lead to additional concerns. For example, some participants mentioned that wearing headphones while using screen readers dampens the sense of hearing and makes it even more difficult to sense their surroundings.

Privacy concerns reported by participants went beyond information privacy to also include projecting a positive image (a privacy concept called *impression management*) in their social and professional lives. Participants reported struggling with various social settings that affected their sense of self, for instance the awkwardness of passing someone in the hall and not knowing whether to greet them as an acquaintance or a stranger, or the embarrassment of trying to talk with someone who has left the room, as one participant mentioned:

> One thing that bothers 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 a fool.

Our participants also expressed concerns related to the "right to be left alone," another influential concept in privacy, although in this case they felt forced to seek help and to engage in interactions they wanted to avoid. Participants reported needing to ask people to help read restaurant menus, fill out forms, find restrooms, and locate personal items. While some of these tasks involved actually divulging confidential information (such as asking a stranger to fill out a medical form), most participants reported that simply having to rely on strangers was a concern in and of itself — they're forced to interact with other people even if they want to keep to themselves.

Our participants (especially those from the urban area) also raised a variety of safety and security concerns related to their visual impairments. Walking outdoors, for instance, can be challenging because they might be unable to recognize potentially unsafe physical and social situations. Participants discussed their fear of walking alone, especially in an unfamiliar neighborhood, and several shared stories of being followed, chased, or mugged, suggesting that their fears aren't unwarranted:

> When I go for walks, I have been followed. And so basically because of how society is today, I don't go for walks with my guide dog because I don't know who is around me and I think that is much more debilitating for me than anything that we have discussed. Not knowing my environment, not knowing who is around me and if something happened to me I would not be able to tell anyone.

To compound the problem, people with visual impairments generally cannot provide an accurate visual description of an assailant to the police, which makes them an even more attractive target for crime.

While our urban participants expressed particular concern about public situations such as walking on streets, taking public transit, and withdrawing money from an ATM, participants from both urban and suburban areas were also concerned even in their own homes:

> I want to know who is coming up to my front door. I hate not knowing that because I feel very vulnerable when people knock at my door at home. We have a home security system on at night but we don't have it on, you know, all the time. That would be horrible to have to unset it to go out and in. We have motion detectors but that hasn't been very optimal either, and I would just like to be warned when somebody is coming up to my porch.

Coping Strategies

Participants described a variety of strategies to alleviate the risks that they expressed. These strategies ranged from completely avoiding certain situations and activities, such as not using computing devices in public places, to devising elaborate mechanisms to overcome lack of full sightedness, such as using echolocation to estimate who was near them and where they were positioned. We classified their strategies into six major categories: avoidance, repositioning, mitigation, assistance from others, adaptation, and acceptance. While most of the defensive strategies were common to both our studies, only urban participants reported using adaptation.

Avoidance

Several concerns could be alleviated by simply avoiding certain situations and behaviors: avoiding walking alone, not using ATM booths, avoiding using computing devices in public, and discouraging social interactions.

Repositioning

Repositioning, or moving to a different place within the environment, was a common defensive strategy. Participants reported that when needing to reveal personal information to someone, they attempted to move to a place where they felt they had privacy. For example, most participants reported requesting a private room before revealing medical details in a doctor's waiting room. A low-vision participant discussed how they handle text messaging on their phone:

> Usually I talk and then stop and go to a corner by myself and send it. Before doing magnification I usually sit somewhere or won't take [the text] right away — I will wait until I am by myself and at the same time put myself back against the wall, so that I am holding my cell phone when I read the text, so that I can see everyone walking around.

But participants also said that repositioning often wasn't possible because of the extra time and effort it requires.

Mitigation

Some participants reported using accessories or programs to defend themselves from nosy bystanders. One common example was to use headphones for screen readers, and another was turning off screens with a screen-curtain program. These strategies, however, don't work for people with low vision impairments who use screen magnification software.

While interacting with others, participants often devised their own mitigation techniques — for example, by talking quickly, quietly, or in an accent. One participant described other strategies:

> With the phone password, sometimes I intentionally make mistakes so that my passwords are a little bit secured. I will hit the keys, I will hit more keys, I will be hitting delete in rapid succession so that it's not easy to understand what the password was ... eventually the password is put in but if it's a four-character password, I actually typed 10 characters including the deletions.

Assistance from Others

For conducting some personal matters, participants reported relying on family members, friends, and even hired personal assistants, but often had to rely on strangers as well. For instance, participants generally seek help from relatives to fill out inaccessible forms and conduct ATM transactions. Although most participants were comfortable with asking for assistance from trusted people, some reported that depending on others always made them uncomfortable.

Adaptation

Participants reported using other senses, such as hearing, to adapt to lack of visual perception. Some reported using echo-location by making clicking sounds and inferring the structure of the local environment based on the echoes, for example, to sense their surroundings. Some participants were able to assess their surroundings by hearing sounds made by nearby people. One participant explained how he uses a smartphone in public:

> I will stop typing if anyone comes closer than three or four feet from me if I am in the grocery store. People tend to stand six or eight feet away from me, but if they approach close to me then I will stop my work and ask them what they are doing. I can tell that because they start to bump into me. I have like a territorial bubble around me and I hear people's footsteps and I hear the activities that are going on behind me. If anyone's presence is near, then they are blocking the sound that I can hear from behind them. It's my "facial vision," they call it, when I hear the echoes. The person's presence blocks the ambient noise.

Acceptance

A final reported coping strategy was simple acceptance of risks associated with their impairment. Some participants felt that the situation was out of their control and that they had little choice but to accept risks. One felt that a person with visual impairment simply couldn't obtain the same level of privacy as sighted people, because they inevitably need to rely on others. Another participant stated that she simply assumes that people are eavesdropping whenever she goes out:

> I guess over my lifetime I have developed an assumption that someone is there. I kind of say to myself, "if I walk out my front door someone can hear me."

Camera-Based Solutions

As we've seen, people with visual impairments face a variety of challenges in managing their physical privacy, safety, and security. They also develop a variety of coping strategies to address these challenges. Although effective, some strategies such as acceptance and avoidance aren't ideal, because they prevent people with visual impairments from realizing the same opportunities that sighted people enjoy.

Based on the concerns and coping strategies we identified, our eventual goal is to devise and inform technology that could help people with visual impairments manage their physical privacy, safety, and security, by providing them with information about their surroundings. We envision a solution that uses cameras to collect images and efficient computer vision algorithms that analyze the images for potential risks. For example, before withdrawing money from an ATM, the device could check the user's surroundings for suspicious people nearby.

Before implementing such a system, it's important to consult potential users to understand the preferences and requirements that might not be evident to system designers. In our study, we discussed the idea of camera-based solutions, and our participants provided valuable feedback about such a system. In this section, we first discuss the types of information that participants desired to help manage privacy, and then discuss other important design considerations for camera-based systems. Our findings could also inform projects in industry that are already underway, including Microsoft's Seeing AI project that detects nearby people and their expressions.[9]

Desired Information

In our study, most of our participants reported that answering a small set of questions would be sufficient to address their major physical privacy, safety, and security concerns.

How many people are in my vicinity? Most participants wished to know the number of people nearby to assess their surroundings and act accordingly. Participants indicated that sensing the exact number of people might not be required, as simply knowing that at least one person is present, or having a rough estimate of the number of people (1 to 3, more than 4, and so on) might be sufficient in many scenarios. Participants said that this information would not only help identify suspicious activity, but also help with navigation.

How close are people to me? Several participants used the term "bubble" to describe the environment immediately surrounding them and expressed the desire to know when people enter or exit their bubble. They reported that knowing the proximity of others is vitally important for assessing surroundings. The radius of the bubble varied between participants, but most imagined 3 to 15 feet. Some participants expressed a desire to divide the area into finer-grained zones, for example, distances of 3 to 6 feet marked high-risk zones, 6 to 10 feet indicated medium risk, and 10 to 15 feet was low risk. The bubble's size might also vary based on context — for example, in public places the bubble might be smaller than in private.

Who's in my vicinity? Participants wanted to identify nearby people, particularly whether they're acquaintances or strangers. Additionally, knowing the identity of people nearby might help participants better manage impressions in social and professional contexts.

What are the people in my vicinity doing? Most participants wished to know the specific activities of others around them, especially if activities are suspicious (for example, someone is staring at them). Knowing others' identity is particularly important in transit stations, doctors' offices, or other public locations. Participants stated that this information could also help them maintain others' privacy by not bothering someone if they knew the other person was busy doing something else.

Who was around me? Some participants suggested an interesting advantage of cameras to help with their safety concerns: the ability to collect evidence. After an incident with crime, police officers need visual descriptions of who was involved and what happened. They suggested preserving a photo record of interactions with other people in case it was later needed. For example, one participant shared an incident on a train where cameras could have been helpful:

> I witnessed at least a couple guys beating up a third guy. I went to my house, and I called 911 and said that I heard this. I described it as best I could, but I could not — they want visuals. If I would have a camera on me anyway … I could just get off the train and I would like to give my phone to the station master and say that here is my camera, you can have it.

Participants also suggested a device that could locate surveillance cameras so that they could make sure the cameras had a clear view when they felt threatened.

Design Considerations

We also asked participants about two important design considerations: camera-based device preference and feedback mechanisms. Our participants reflected on the camera-based technology and offered further suggestions. Their suggestions of design attributes fell into four categories.

Discretion. Participants said discreetness is a key requirement, so that the device itself doesn't draw additional attention. This is important not only for aesthetic reasons, but also so that the devices don't draw a potential attacker's attention.

Wearability. Most participants preferred wearable devices over other form factors (such as handheld), for reasons including that they would be less noticeable and more convenient by not requiring deliberate actions such as aiming a smartphone. Some participants hoped that the cameras could be as small as a lapel pin or an earring. Although some participants preferred head-mounted cameras, others worried they wouldn't be discreet or would look "weird."

Subtle feedback. How the device should provide information about the environment is another important design consideration mentioned by participants. Most participants felt the mechanism should be discreet and shouldn't draw additional attention: simple audio or haptic feedback (such as vibrations), for example.

Forensic considerations. As mentioned earlier, our participants reported wanting to use cameras for forensic purposes. They mentioned two possible operating modes: a normal mode in which the system collects photos only occasionally, and a safety mode in which it collects photos in short intervals. Images from the safety mode could then be used for forensic purposes. They desired a way to explicitly switch between modes, either manually or automatically based on a policy specified ahead of time (for example, if a loud noise is detected).

Our study clarifies that people with visual impairments struggle to manage their physical privacy, safety, and security. They face numerous risks in their daily lives, and although some of these risks are common to everyone, they're heightened by visual impairments. Although our participants have coping strategies to manage concerns, we've seen that some strategies still put them at risk (acceptance) or prevent them from doing certain things (avoidance). Overall, participants expressed their desire for better tools to address these problems and concerns.

This study is an initial step toward such a solution. We've made progress in understanding requirements and have better knowledge of what information is important in managing privacy, as well as how camera-based systems should be designed and under which circumstances they would be appropriate. We still need to understand how devices could accurately detect this information, and how best to communicate it to the user. Recent progress on computer vision-based techniques seems promising, but more research is required to understand how to infer useful information from images.

Our envisioned camera-based approach isn't likely to solve all privacy concerns, but it has the potential to help people with visual impairments better manage them. Moreover, it might help with coping strategies. Participants using repositioning and mitigation strategies could save time and effort by knowing if anyone is around, for example, when looking for a private location in a public place.

Our study was qualitative and any differences between groups would need quantitative validation. Nevertheless, we highlight a few themes we observed based on the participants' backgrounds and demographics. First, our participants from urban areas were much more concerned about safety and security than privacy, and thus urban populations might be more interested in the forensic capabilities of such devices. We explored whether concerns were associated with particular types of impairments or gender, but our interviews indicate that the concerns are more likely to be associated with personal history and experience. For example, although we observed a trend of female participants being more concerned about their safety (9 of 19), three (among 14) males expressed heightened safety concerns due to personal experience with being mugged.

We view this work as an initial step, and we hope that it motivates others to consider the problems of people with visual impairments and help devise solutions that might improve their lives.

Acknowledgments
This material is based upon work supported by the US National Science Foundation under awards CNS-1408730 and IIS-1253549. We thank our participants for taking part in our study.

References

1. B. Silverstone et al., *The Lighthouse Handbook on Vision Impairment and Vision Rehabilitation*, Oxford Univ. Press, 2000.
2. M. Hersh and M.A. Johnson, *Assistive Technology for Visually Impaired and Blind People*, 1st ed., Springer, 2008.
3. S. Azenkot et al., "Passchords: Secure Multi-Touch Authentication for Blind People," *Proc. 14th Int'l ACM Sigaccess Conf. Computers and Accessibility*, 2012, pp. 159–166.
4. S.K. Kane et al., "Freedom to Roam: A Study of Mobile Device Adoption and Accessibility for People with Visual and Motor Disabilities," *Proc. 11th Int'l ACM Sigaccess Conf. Computers and Accessibility*, 2009, pp. 115–122.
5. T. Ahmed et al., "Privacy Concerns and Behaviors of People with Visual Impairments," *Proc. 33rd Ann. ACM Conf. Human Factors in Computing Systems*, 2015, pp. 3523–3532.
6. T. Ahmed et al., "Addressing Physical Safety, Security, and Privacy for People with Visual Impairments," *Proc. 12th Symp. Usable Privacy and Security*, 2016, pp. 341–354.
7. J.R. Terven, J. Salas, and B. Raducanu, "New Opportunities for Computer Vision-Based Assistive Technology Systems for the Visually Impaired," *Computer*, vol. 47, no. 4, 2014, pp. 52–58.
8. J.P. Bigham et al., "VizWiz: Nearly Real-Time Answers to Visual Questions," *Proc. 23rd Ann. ACM Symp. User Interface Software and Technology*, 2010, pp. 333–342.
9. V. Rao, "Seeing AI: Microsoft Project for Blind People That Lets Them 'See,'" 2016; http://assistivetechnologyblog.com/2016/03/seeing-ai-microsoft-project-for-blind.html.

Tousif Ahmed is a PhD candidate in the School of Computer Science at Indiana University Bloomington. His research interests include usable security and privacy. Ahmed has a BS in computer science and engineering from the Bangladesh University of Engineering and Technology. Contact him at touahmed@indiana.edu.

Roberto Hoyle is an assistant professor in the Department of Computer Science at Oberlin College. His research interests include security and privacy. Hoyle has a PhD in computer science from Indiana University Bloomington. Contact him at rjhoyle@oberlin.edu.

Patrick Shaffer is a second-year PhD student in the School of Informatics and Computing at Indiana University Bloomington. His research interests include data mining, artificial intelligence, and social networks. Shaffer has an MS in astronautical engineering from the Naval Postgraduate School. Contact him at patshaff@indiana.edu.

Kay Connelly is an associate professor in the School of Informatics and Computing at Indiana University Bloomington. Her research interests include user acceptance of ubiquitous and mobile computing technologies where there is a delicate balance between such factors as convenience, control, and privacy. Connelly has a PhD in computer science from the University of Illinois at Urbana-Champaign. Contact her at connelly@indiana.edu.

David Crandall is an associate professor in the School of Informatics and Computing at Indiana University Bloomington. His research interests include computer vision, machine learning, and data mining. Crandall has a PhD in computer science from Cornell University. He's the recipient of a US National Science Foundation CAREER award and a Google Faculty Research Award. Contact him at djcran@indiana.edu.

Apu Kapadia is an associate professor at the School of Informatics and Computing at Indiana University Bloomington. His research interests include security and privacy and particularly pervasive, mobile, and wearable computing; human factors; accountable anonymity; crowdsourcing; and peer-to-peer networks. Kapadia has a PhD in computer science from University of Illinois at Urbana-Champaign. He has received five US National Science Foundation grants, including a CAREER award in 2013 and a Google Research Award in 2014. He's a member of ACM and IEEE. Contact him at kapadia@indiana.edu.