Privacy Risks of Using Camera Assisted Tools for People with Visual Impairments

Anonymous CVPR submission

Paper ID ****

Abstract

Computer vision and augmented reality devices are soon to enter the market, and they have great potential to improve the lives of people with visual impairments. However, there are privacy risks associated with camera-assisted devices for people with visual impairments. We conducted three interviews with 47 people with visual impairments, where the participants mentioned three specific privacy concerns (sharing sensitive information in error while taking photos) with cameras along with other general privacy concerns. We report the privacy concerns and discuss different ways to address (hiding details from image) these concerns.

1. Introduction

The advancement of computer vision and augmented reality technologies have opened a new era to build assistive technologies for people with visual impairments. Various assistive technologies, such as Aipoly[1], Orcam[2], Google glass[3], and other camera assisted devices and applications, are emerging to help people with visual impairments sense the world around them in real time using computer vision and augmented reality. With the emergence of augmented reality and virtual reality devices, it is expected that these devices will make the world more accessible for people with visual impairments [4]. However, the emerging usage of cameras on the new devices may also create privacy risks. For example, while using cameras, a visually impaired user may capture sensitive information unintentionally and possibly share it with public. Along with accessibility issues, it is important to consider the privacy risks.

In this abstract, we discuss the privacy issues with camera-based devices and applications that arose during our three studies involving 47 participants with visual impairments. In our first study, we interviewed 14 people with visual impairments to explore the general privacy concerns of people with visual impairments while interacting in the physical and virtual world, along with their privacy concerns while they interact with computing devices [1]. In our second study, we conducted a follow-up study with 19 participants with visual impairments and asked their opinion of a camera-based assistive tool which may address most of their privacy concerns [2]. In the third study, we implemented three prototypes for helping them interact with a camera-assisted tool and receive feedback about their surroundings. In our studies, our participants discussed their interaction with cameras several times and raised several privacy concerns. In this abstract, we report three privacy issues of camera-assisted devices that were raised by our participants and discuss some potential approaches to address the issues.

[1] aipoly.com
[2] www.orcam.com/
[3] www.google.com/glass

2. Privacy Risks of Cameras

In this section, we discuss the privacy risks that can arise due to the use of cameras on vision and AR-based systems. These issues show that more caution is required when designing an accessible solution for people with visual impairments who use augmented reality devices. We also discuss different ways to mitigate the privacy risks.

2.1. Misclosure

A *Misclosure* occurs when people mistakenly expose private information [3]. As computer vision-based technologies are not yet fully automated, human crowd workers are sometimes added to the assistive system to help people with visual impairments. As people with visual impairments face difficulties taking a good photo and usually don't know the image content, they can often capture sensitive information and might inadvertently expose those information to crowd workers. In our second study, one participant reported an incident where she accidentally exposed a nude photo of herself to a crowd worker while trying to differentiate between a shampoo and a conditioner in a hotel room because she was unaware of the mirror in the wash room. As the visually impaired cannot identify whether the captured image contains

sensitive information or not, there is always a risk associated with using cameras. Even if the system is automated and uses cloud-based services, the risk may still exist since collected data can be exposed. Moreover, as people with visual impairments are using social media and uploading photos, they may share images containing unintended objects with their friends and family.

Researchers and developers may prevent such situations by incorporating additional measures while implementing a camera based system. Jana et al. [6] proposed scanner darkly system to add a privacy layer with the OpenCV applications and showed that the functionality of the camera applications can be sustained by removing unimportant details. By segmenting different objects in a photo and then filtering them later *Misclosure* incidents can possibly be averted. If it is required to send an image to crowd workers, then the system can also inform the user about the risks.

2.2. Unwanted Exposure

The assistive tools currently incorporated with regular devices are often multifunctional with visual interfaces. The additional functionality adds user friendliness for a sighted person but sometimes can cause discomfort to people with visual impairment. Most mobile and ubiquitous devices feature cameras and microphones which can continuously monitor the surrounding environments for input. Templeman et al. [7] showed that cameras of mobile devices can surreptitiously take photos in the background, and an attacker can gain sensitive information through those photos. To prevent such situations, the privacy indicator a green light to indicate the camera is on can be used, but it is not often helpful for people with visual impairments.

The unwanted exposure can be averted by following a simple design consideration. There can be a physical camera blocker with all devices so that people with visual impairments can easily block the camera.

2.3. Bystander Privacy Violation

In the near future, camera-based tools and augmented reality devices could be used to give information to visually impaired people about their surroundings. One approach for such a system is to observe the environment through cameras, then analyze the data and give them the information about the environment. While presenting a camera-based tool to our participants, several participants raised the issue of bystanders' privacy. While sensing data from the environment, the device may also collect sensitive information from bystanders and potentially reveal it to other people. Moreover, the bystanders have an expectation of privacy while they interact with people with visual impairments. Exposing the bystanders' information to visually impaired people may violate bystanders' privacy. Therefore, the bystander may feel uncomfortable when these assistive technologies are in use [5].

One solution for this issue is to limit the capabilities of such devices. For a sighted person, there is a boundary on observing a scenario at a particular moment. But if a camera is used to observe the 360-degree environment around a person, then it often breaks the natural flow and hampers the privacy of the bystanders around the user. Therefore, the devices can be limited to normal viewing angles. There can be a trade-off between privacy and utility here, however, and more research is required to address this issue.

3. Conclusion

Computer vision and augmented reality based assistive technologies are evolving radically to improve the quality of life and independence of people with visual impairment. However, more attention must be given while designing these tools due to the several privacy risks associated with them. In this abstract, we have presented several privacy concerns associated with the camera-based assistive technology, and we believe there are many others which provide sufficient motivations to focus more on including privacy in the early design process for the assistive devices.

References

[1] T. Ahmed, R. Hoyle, K. Connelly, D. Crandall, and A. Kapadia. Privacy concerns and behaviors of people with visual impairments, 2015. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (pp. 3523-3532). ACM. 1

[2] T. Ahmed, P. Shaffer, K. Connelly, D. Crandall, and A. Kapadia. Addressing physical safety, security, and privacy for people with visual impairments. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 341–354, Denver, CO, June 2016. USENIX Association. 1

[3] K. E. Caine. Supporting privacy by preventing misclosure, 2009. In Extended Abstracts on Human Factors in Computing Systems (pp. 3145-3148). ACM. 1

[4] J. Carmigniani, B. Furht, M. Anisetti, P. Ceravolo, E. Damiani, and M. Ivkovic. Augmented reality technologies, systems and applications, 2011. Multimedia Tools and Applications, 51(1), pp.341-377. 1

[5] T. Denning, Z. Dehlawi, and T. Kohno. In situ with bystanders of augmented reality glasses: Perspectives on recording and privacy-mediating technologies, 2014. In Proceedings of the 32^{nd} annual ACM conference on Human factors in computing systems (pp. 2377-2386). ACM. 2

[6] S. Jana, A. Narayanan, and V. Shmatikov. A scanner darkly: Protecting user privacy from perceptual applications, 2013. In Security and Privacy (SP), IEEE Symposium on (pp. 349-363). IEEE. 2

[7] R. Templeman, Z. Rahman, D. Crandall, and A. Kapadia. Placeraider: Virtual theft in physical spaces with smartphones, 2012. arXiv preprint arXiv:1209.5982. 2