# Surveillance Considerations Concerning Assistive Devices for People with Visual Impairments

**Patrick Shaffer**
Schoold of Informatics
Indiana University
patshaff@indiana.edu

**Kay Connelly**
School of Informatics
Indiana University
connelly@indiana.edu

**Tousif Ahmed**
School of Informatics
Indiana University
touahmed@indiana.edu

**David Crandall**
School of Informatics
Indiana University
djcran@indiana.edu

**Roberto Hoyle**
School of Informatics
Indiana University
rjhoyle@indiana.edu

**Apu Kapadia**
School of Informatics
Indiana University
kapadia@indiana.edu



## Abstract
The use of cameras to assist persons with visual impairments is rapidly becoming realizable. However, the surveillance implications of cameras as assistive devices present unintended effects which must be considered during the design of an assistive system. During a recent study of persons with visual impairments, a significant number of those persons in the study desired a forensics capability to accompany their camera so that they can have a record of harmful events that they could share with either a trusted agent or law enforcement. Incorporating a forensics feature into an assistive device presents an opportunity for social good as well as potential harm in the form of surveillance.

## Introduction
A recent study [1] by our team that queried 19 persons with visual impairments about their preferences concerning the design of a notional assistive device that enhanced their privacy showed some interesting results. A significant number of our participants indicated that while they had privacy concerns about eavesdropping and shoulder surfing, they were more concerned over their safety. In particular, several of our participants related experiences where they were either victims of a crime or had witnessed a crime but were unable to describe the assailants because of their visual impairment. These users

specifically asked for a feature in the assistive device that would allow them to save a visual record of a negative event with the specific purpose of sharing the information with law enforcement or a trusted agent.

*Record, Forward and Store*
A notional assistive device uses a camera and perhaps other sensors to notify a person with a visual impairment of the presence of others in proximity to them so that they can better manage their personal safety and privacy. With the incorporation of a forensics capability, the assistive device could switch to a mode where visual information is recorded and forwarded to the cloud (for example) for real time analysis by a trusted agent or for post event review by law enforcement. The addition of this *forensics* capability directly addresses the concerns brought up by our participants and also preserves the record independent of the assistive device should it be lost or stolen. Products such as Aira IO[1] and Emergensee[2] combine the use of streaming video and a trusted agent to assist their target customers.

*Creation of a New Surveillance Node*
Preserving camera information for the record in order to assist persons with visual impairments is an example of the employment of technology for social good and supports surveillance of the most vulnerable; however, it also results in the creation of another surveillance node for which design for privacy must be considered to prevent inadvertent misclosures [2] of either the wearer's or bystanders' visual privacy. While the intent of the assistive device is altruistic, it can also be construed as something similar to a lifelogging device and applicable lessons learned apply [3]. Finally, in worst case, the camera and its data stream could be adulterated or redirected to entities with malicious intent. Designers of assistive devices need to be mindful of the impact of privacy upon both the targeted user population as well as the general public and should design privacy and security into the device up front.

[1] www.aira.io
[2] www.emergensee.com

## Conclusion
As camera based assistive devices for the visually impaired become realizable, system designers, users and practitioners need to be mindful of the privacy considerations that this new surveillance mode brings, particularly when the camera data stream is preserved for the record. We argue that the privacy considerations need to be designed into the system from the start rather than treated as an afterthought in order to mitigate some of the concerns identified during lifelogging or from malicious entities.

## Acknowledgements
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. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

## References
[1] Ahmed, T., Hoyle, R., Connelly, K., Crandall, D., and Kapadia, A. Privacy concerns and behaviors of people with visual impairments. In *Proceedings of The ACM SIGCHI Conference on Human Factors in Computing Systems (CHI '15)* (Apr. 2015), 3523–3532.

[2] Caine, K. E. Supporting privacy by preventing misclosure. In *Extended Abstracts on Human Factors*

*in Computing Systems*, CHI EA '09, ACM (New York, NY, USA, 2009), 3145–3148.

[3] Hoyle, R., Templeman, R., Armes, S., Anthony, D., Crandall, D., and Kapadia, A. Privacy behaviors of lifeloggers using wearable cameras. In *Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp)* (Sept. 2014), 571–582.