New tech addresses augmented reality's privacy problem

January 17 2024, by Kelly Izlar

(From left) Bo Ji, Brendan David-John, and graduate student Matthew Corbett devised a new method to protect bystander privacy in augmented reality. Credit: Kelly Izlar/Virginia Tech

An emergency room doctor using augmented reality could save precious

seconds by quickly checking a patient's vitals or records. But the doctor could also unintentionally pull information for someone else in the room, breaching privacy and health care laws.

A Commonwealth Cyber Initiative team created a technique called BystandAR to protect bystander privacy while still providing an immersive augmented-reality experience. The researchers presented the technology at ACM MobiSys 2023 last summer and explained it in a December *IEEE Security & Privacy* article.

"Protecting bystander privacy is an important problem," said Bo Ji, associate professor of computer science. "Our work raises awareness and encourages the adoption of augmented reality in the future."

Early results, which were presented last summer, correctly identified and protected more than 98% of bystanders within the data stream while allowing access to more than 96% of the subject data. In addition, BystandAR does not require offloading unprotected bystander data to another device for analysis, which presented a further risk for privacy leakage.

With support from Virginia Tech Intellectual Properties and the LINK + LICENSE + LAUNCH Proof of Concept Program, the team filed a provisional patent on BystandAR, which distorts bystanders' images in augmented-reality devices.

Concerns about privacy violations contributed to the failure of Google Glass almost a decade ago. Like similar devices, the eyewear projects interactive computer-generated content, such as video, graphics, or GPS data, onto a user's view of the world. But Google Glass' cameras and microphones allowed users to record their surroundings without the consent of those around them.

"It made people uncomfortable, and for good reason," Ji said. "Maybe you're in a restaurant with your kids. You have no control over who is collecting their data or what happens to it."

BystandAR builds on a key insight from psychological studies: An individual usually looks most directly and longest at the person they are interacting with. Therefore, eye gaze is a highly effective indicator for differentiating between bystander and subject in a social context. Ji's technique leverages eye-gaze tracking, near-field microphone, and spatial awareness to detect and obscure bystanders captured within sensor data in real time.

In a related work, for which he recently received a $1.2 million National Science Foundation award, Ji is developing a method to improve the efficiency and performance of next-generation wireless networks so that more people can take advantage of seamless, immersive augmented reality experiences.

"Although these are two separate projects, you can think of it as a part of the same effort to improve augmented reality from both sides—ensuring privacy for individual users locally, and improving the network to provide a seamless, secure, and functional experience globally," Ji said.

More information: Matthew Corbett et al, Securing Bystander Privacy in Mixed Reality While Protecting the User Experience, *IEEE Security & Privacy* (2023). DOI: 10.1109/MSEC.2023.3331649

Matthew Corbett et al, BystandAR: Protecting Bystander Visual Data in Augmented Reality Systems, *Proceedings of the 21st Annual International Conference on Mobile Systems, Applications and Services* (2023). DOI: 10.1145/3581791.3596830

Provided by Virginia Tech