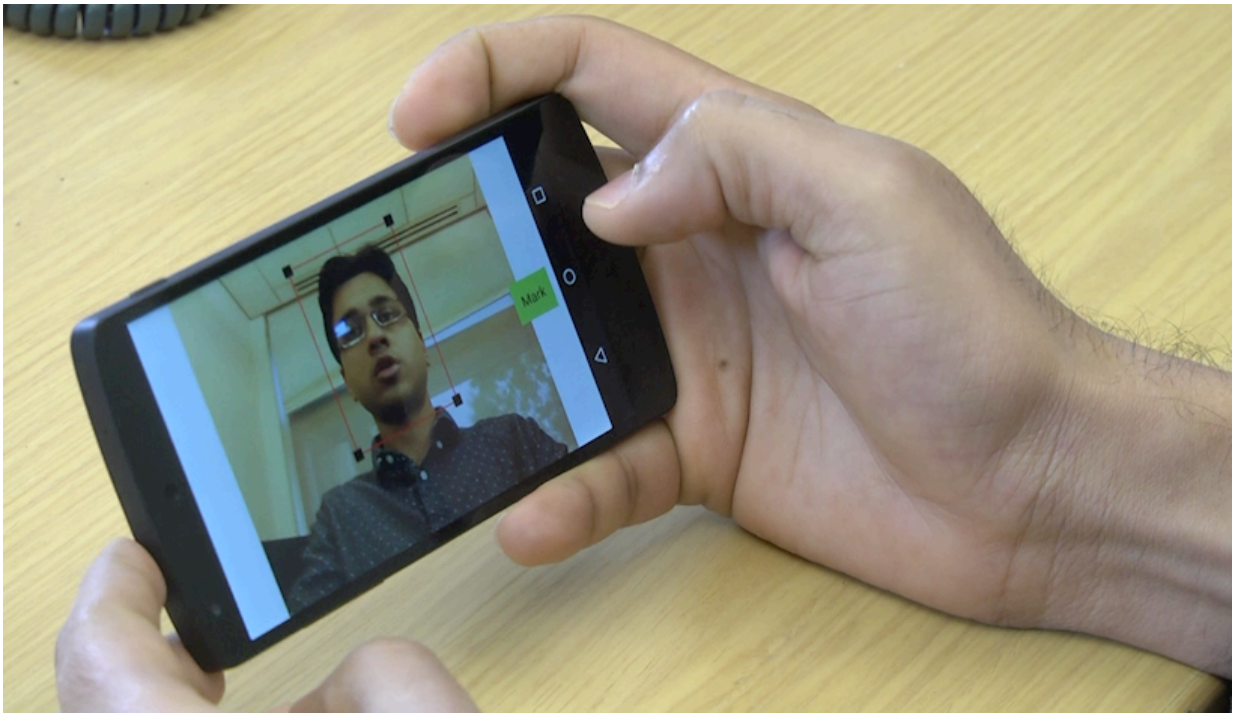
Video privacy software lets you select what others can see

June 28 2016, by Robin A. Smith



Video privacy software developed at Duke lets users select the part of a scene that is OK to share by drawing a rectangular border around it, either by hand or with a few clicks of a mouse. Credit: Julie Schoonmaker, Duke University

Camera-equipped smartphones, laptops and other devices make it possible to share ideas and images with anyone, anywhere, often in real-time. But in our cameras-everywhere culture, the risk of accidentally leaking sensitive information is growing.

Computer scientists at Duke University have developed software that helps prevent inadvertent disclosure of trade secrets and other restricted information within a camera's field of view by letting users specify what others can see.

A video chat with collaborators, customers or suppliers outside of the office, for example, could reveal confidential product plans drawn on a whiteboard in the background, or sales figures or source code on nearby computer screens.

Using a smartphone to scan a receipt for expense purposes could also expose portions of meeting notes, pill bottles, and other personal items on your desk.

"There are more and more cameras every year. They're incredibly useful," said Landon Cox, an associate professor of computer science at Duke. "But the downside is we're now converting large swaths of our surroundings to a digital format that's easy to access and share, including things we might not want to be digitizing."

The simplest way to ensure privacy is to disable the camera or microphone when sensitive information is in the frame, Cox said.

But rather than all or nothing, the researchers wanted to give users more granular control over which objects in the camera's view are shared and which are kept private.

Prior efforts to safeguard confidential information in photos and video use a "blacklist" approach. Developers anticipate things that users might want to hide, and build software that blurs or masks them in each frame.

But coming up with an exhaustive list of potentially troublesome objects is virtually impossible. "Things that some people consider sensitive

might not be sensitive to you," said assistant professor of computer science Ashwin Machanavajjhala, who co-authored the research. "It's hard to build something that covers all possible scenarios."

Even for objects that security technology has blacklisted in advance, building software that detects and conceals them quickly and consistently under changing light conditions and motion-induced blur has proven challenging.

"Even if it fails just 1 or 2 percent of the time, it's not secure," said co-author Animesh Srivastava, a graduate student at Duke.

So the team tried a different strategy. Instead of relying on a developer's best guesstimate of which objects should be "public" and which should be "private," the researchers set things up so that the user makes that determination. And instead of choosing what to hide, the user chooses what to reveal.

"If we get it right, hopefully it will lead to something that's more secure and easier to use," Cox said.

The researchers presented two examples of their approach on June 28 at the 14th International Conference on Mobile Systems, Applications, and Services (MobiSys 2016) in Singapore.

One is designed to protect sensitive information on two-dimensional surfaces such as whiteboards and computer presentation slides. The other safeguards images of three-dimensional objects such as keyboards and faces.

In both cases, users select the part of a scene that is OK to share by drawing a rectangular border around it, either by hand or with a few clicks of a mouse.

Once it knows what it's looking for, the software intercepts all incoming frames from the video stream and rapidly scans frame by frame for a match using computer vision technology.

Only authorized objects are allowed to pass from the camera to third-party software, like smartphone apps. Everything else is blocked out by default.

"The key challenges in designing these systems were to ensure that the marking process was easy for the users, and that detecting public regions did not slow down the camera output or the smartphone," Machanavajjhala said.

In one user study, the researchers asked 26 people to use Android smartphones to scan QR codes—the square-shaped barcodes that are becoming increasingly popular in ads—with and without the new security features. The participants rated the speed and ease of the cameras on the "secure" smartphones on par with unmodified smartphones.

The team also tested their security software on videos shot when the camera was in motion. They found they could reliably safeguard sensitive regions while still delivering 24 frames per second, fast enough for human eyes to perceive a smooth moving picture rather than a flickering image on a screen.

This isn't the ultimate solution to image privacy protection, Machanavajjhala said. The software doesn't protect things caught by cameras outside a person's control, for example. "If you're just walking around on the street, and you want to ensure that your face isn't captured, this won't work," he said.

But in the future, the team hopes their research will encourage

technology companiesto design and develop products that give users more privacy when it comes to their own devices.

In the meantime, they are looking into ways of giving users similarly fine-grained privacy controls over audio recordings in addition to images, by allowing third parties to hear only certain voices, words or noises in an audio stream, for example.

"People are going to want some way to control the information that things like microphones and motion detectors and other sensors have access to in a much smarter way than just turning them on or off," Cox said. "These kinds of issues are going to be really important to figure out over the next decade."

More information: "What You Mark is What Apps See," Nisarg Raval, Animesh Srivastava, Ali Razeen, Kiron Lebeck, Ashwin Machanavajjhala and Landon Cox. MobiSys'16, June 25-30, 2016, Singapore. DOI: 10.1145/2906388.2906405

Provided by Duke University