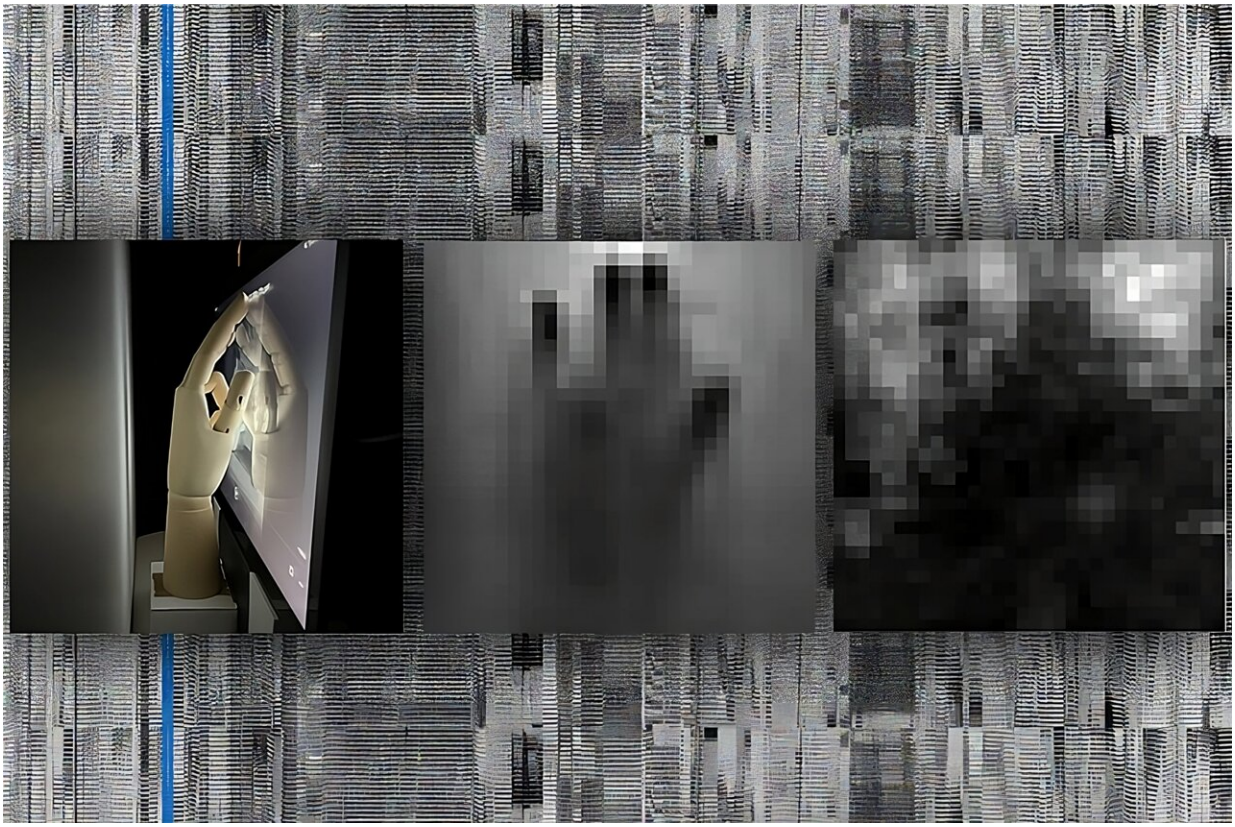
Smart devices' ambient light sensors pose imaging privacy risk

January 17 2024, by Alex Shipps



CSAIL uncovered that ambient light sensors are vulnerable to privacy threats when embedded on a smart device's screen. Credit: Alex Shipps/MIT CSAIL

In George Orwell's novel "1984," Big Brother watches citizens through two-way, TV-like telescreens to surveil citizens without any cameras. In

a similar fashion, our current smart devices contain ambient light sensors, which open the door to a different threat: Hackers.

These passive, seemingly innocuous smartphone components receive light from the environment and adjust the screen's brightness accordingly, like when your phone automatically dims in a bright room. Unlike cameras, though, apps are not required to ask for permission to use these sensors.

In a surprising discovery, researchers from MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL) uncovered that ambient light sensors are vulnerable to privacy threats when embedded on a smart device's screen.

The team proposed a computational imaging algorithm to recover an image of the environment from the perspective of the display screen using subtle single-point light intensity changes of these sensors to demonstrate how hackers could use them in tandem with monitors.

The paper was published in *Science Advances* earlier this January.

"This work turns your device's ambient light sensor and screen into a camera! Ambient light sensors are tiny devices deployed in almost all portable devices and screens that surround us in our daily lives," says Princeton University professor Felix Heide, who was not involved with the paper. "As such, the authors highlight a privacy threat that affects a comprehensive class of devices and has been overlooked so far."

While phone cameras have previously been exposed as security threats for recording user activity, the MIT group found that ambient light sensors can capture images of users' touch interactions without a camera. According to their new study, these sensors can eavesdrop on regular gestures, like scrolling, swiping, or sliding, and capture how users

interact with their phones while watching videos. For example, apps with native access to your screen, including video players and web browsers, could spy on you to gather this permission-free data.

According to the researchers, the commonly held belief is that ambient light sensors don't reveal meaningful private information to hackers, so programming apps to request access to them is unnecessary. "Many believe that these sensors should always be turned on," says lead author Yang Liu, MIT Electrical Engineering & Computer Science Department (EECS) and CSAIL Ph.D. student.

"But much like the telescreen, ambient light sensors can passively capture what we're doing without our permission, while apps are required to request access to our cameras. Our demonstrations show that when combined with a display screen, these sensors could pose some sort of imaging privacy threat by providing that information to hackers monitoring your smart devices."

Collecting these images requires a dedicated inversion process where the ambient light sensor first collects low-bitrate variations in light intensity, partially blocked by the hand making contact with the screen. Next, the outputs are mapped into a two-dimensional space by forming an inverse problem with the knowledge of the screen content. An algorithm then reconstructs the picture from the screen's perspective, which is iteratively optimized and denoised via deep learning to reveal a pixelated image of hand activity.

The study introduces a novel combination of passive sensors and active monitors to reveal a previously unexplored imaging threat that could expose the environment in front of the screen to hackers processing the sensor data from another device. "This imaging privacy threat has never been demonstrated before," says Liu, who worked alongside Frédo Durand on the paper, who is an MIT EECS professor, CSAIL member,

and senior author.

The team suggested two software mitigation measures for operating system providers: tightening up permissions and reducing the precision and speed of the sensors. First, they recommend restricting access to the ambient light sensor by allowing users to approve or deny those requests from apps. To further prevent any privacy threats, the team also proposed limiting the capabilities of the sensors.

By reducing the precision and speed of these components, the sensors would reveal less private information. From the hardware side, the ambient light sensor should not be directly facing the user on any smart device, they argued, but instead placed on the side where it won't capture any significant touch interactions.

Getting the picture

The inversion process was applied to three demonstrations using an Android tablet. In the first test, the researchers seated a mannequin in front of the device, while different hands made contact with the screen. A human hand pointed to the screen, and later, a cardboard cutout resembling an open-hand gesture touched the monitor, with the pixelated imprints gathered by the MIT team revealing the physical interactions with the screen.

A subsequent demo with human hands revealed that the way users slide, scroll, pinch, swipe, and rotate could be gradually captured by hackers through the same imaging method, although only at a speed of one frame every 3.3 minutes. With a faster ambient light sensor, malicious actors could potentially eavesdrop on user interactions with their devices in real time.

In a third demo, the group found that users are also at risk when

watching videos like films and short clips. A human hand hovered in front of the sensor while scenes from Tom and Jerry played on screen, with a white board behind the user reflecting light to the device. The ambient light sensor captured the subtle intensity changes for each video frame with the resulting images exposing touch gestures.

While the vulnerabilities in ambient light sensors pose a threat, such a hack is still restricted. The speed of this privacy issue is low, with the current image retrieval rate being 3.3 minutes per frame, which overwhelms the dwell of user interactions. Additionally, these pictures are still a bit blurry if retrieved from a natural video, potentially leading to future research. While telescreens can capture objects away from the screen, this imaging privacy issue is only confirmed for objects that make contact with a mobile device's screen, much like how selfie cameras cannot capture objects out of frame.

More information: Yang Liu et al, Imaging privacy threats from an ambient light sensor, *Science Advances* (2024). DOI: 10.1126/sciadv.adj3608

Provided by Massachusetts Institute of Technology