

Hackers Got Inside a Flock Camera. Its Data Shows How the System Really Works

Dhruv Mehrotra, Joseph Cox

Hackers ripped down a [Flock camera](#) above a roadway, made a near-complete copy of the data stored inside it, and shared the files with [404 Media](#) and WIRED, revealing in new detail how exactly Flock Safety's cameras track the movements of [both vehicles and people](#). The hackers say they are also publishing details on how they managed to obtain the software, in the hopes that other people may copy them.

The breach provides an unprecedented look inside a system that Flock has described as protected by [on-device encryption](#). The hackers were able to copy the camera's storage and recover an encryption key stored on the device, which unlocked videos of thousands of vehicle detections. The hackers shared the material with 404 Media and the transparency nonprofit Distributed Denial of Secrets, which shared the data with WIRED. 404 Media and WIRED then analyzed those files as part of a joint investigation.

While much of the automatic license plate reader's most sensitive storage remained encrypted and inaccessible, the joint analysis of the recovered data shows that software running on the device explicitly detects people as well as vehicles, license plates, and bicycles. The camera can produce dozens of images of a single passing vehicle and, according to several weeks of recovered logs, generated more than a million images. Its computer-vision software also sometimes isolated bumper stickers and other graphics, including, in one case, an American flag patch on a motorcyclist's saddlebag.

The act of removing the camera and dumping its software shows that some people are not content with just destroying or removing the cameras. Across the country, multiple people have been arrested for allegedly tampering with or otherwise sabotaging Flock's cameras. In response, some towns have announced that they are going to stop using Flock's cameras altogether, and in one case, a police department even [made a fake, 3D-printed Flock camera case](#) in order to bait potential vandals.

"Why just destroy them when we can reverse engineer them and find the secrets of those spying on us?" one of the hackers, from a collective calling itself stegan0gram, said in an interview. "We liberated hardware in the field, disarmed them, and proceeded with reverse engineering of the cameras and associated solar equipment."

Flock's cameras photograph passing vehicles and send the images and other data to the company's servers. There, Flock's system presumably reads the license plate and can identify characteristics such as the vehicle's color, make, and model. Flock then makes these time-stamped records searchable by whichever local agency owns or has access to the cameras. But in many cases, Flock's system also allows other police departments from all over the country to search those cameras too, as part of the company's national network. In Alpharetta, Georgia, for example, [WIRED found](#) that records from the city's Flock cameras were accessible to more than 2,000 agencies, including police departments, colleges, airports, and, inexplicably, the Office of Inspector General for the federal General Services Administration.

This national network has been a selling point for Flock but also a deep source of controversy. [404 Media revealed](#) that local cops were performing lookups in the national network on behalf of Immigration and Customs Enforcement, including in areas that banned working with immigration authorities or [transferring license plate data](#) out of state. [404 Media also revealed](#) that a cop in Texas searched Flock cameras nationwide for a woman who self-administered an abortion. Those stories, among others, triggered a national conversation about whether people want Flock cameras, or automatic license plate readers more generally, in their communities.

And in the case of stegan0gram, the answer is clearly no.

The hackers said they were able to access the Android system on the camera and found two partitions—sections of its hard drive, essentially. A few of these were unencrypted, the hackers said, including one called “vendor” and another called “media.” The latter contained an encryption key that unlocked another part, which contained much of the media—the videos and stills—the camera took.