

Congress has failed to regulate Flock cameras to prevent surveillance

Translate

By Catherine Crump
Los Angeles Times

Vigilantes are disabling Flock cameras in at least three dozen states, and although I don't condone property damage, I understand the outrage. The American people did not ask for a sprawling nationwide surveillance apparatus operated in secret and subject to few rules. Our elected representatives did not vote for this. These systems' potential for abuse is vast, and law enforcement's treatment of the data they generate has been careless. Foisting these systems on the public is Silicon Valley's now-familiar "move fast and break things" arrogance — applied, this time, to the norms of democratic governance.

Flock Safety is just one of several automated license plate reader camera systems, although it has quickly come to dominate the market. The company estimates 5,000 law enforcement agencies use its products — although the Los Angeles Police Department no longer numbers among them, having stopped working with Flock in July because of privacy concerns.

These systems photograph every passing car, convert the license plate number to machine-readable text, and store and geotag the image. Law enforcement agents can then look up plates or even identify all plates that were in a particular location at a specific time. Establish a dense enough network of cameras, and it becomes possible to track people through their daily lives.

A key fact: These systems don't just capture images of people wanted for a crime. They store photos of everyone. It's a tool of mass, indiscriminate surveillance. In 2020, a California state auditor's report found that of the 320 million images the Los Angeles Police Department had stored, 99.9% were of vehicles that were not on a hot list.

I'm not opposed to license plate readers. Used well, they can help solve crimes and improve public safety by flagging stolen cars or vehicles associated with people wanted for felonies.

But they're also vulnerable to abuse. After 9/11, New York police drove license-plate-reader-equipped cars past mosques to record worshippers' vehicles. In 2015 two federal agencies planned to use them at gun shows. This May, a Texas sheriff's office searched 83,000 cameras for a woman who had an abortion. Last year, a privacy advocacy group combing through audit logs revealed that California police were sharing data with ICE — in violation of state law. And individual officers have abused these systems, including a Georgia police chief who looked up the plates of his ex-girlfriend and her daughter some 600 times.

Too many law enforcement agencies have been careless with the data of Americans who are not under investigation. Any competent auditing system would flag an officer searching for the same plate hundreds of times, as happened in Georgia. If a small band of volunteers can figure out that California police and sheriffs are violating state law, surely these agencies can develop their own internal audit mechanisms. But it's hard to believe they have the will to do so.

Until recently, elected officials mostly haven't scrutinized these systems. They should be having a real debate about the place of this technology in our communities. Should plate readers be installed at all? How long should data be stored if it isn't related to someone suspected of criminal activity? Should law enforcement have to obtain a warrant to query the database?

What shouldn't be happening is a de facto nationwide private surveillance system cobbled together without any democratic mandate. Some city councils may have approved plate readers locally, but the whole is greater than the sum of its parts — and elected officials have not been voting on whether to build a vast nationwide database.

Perhaps this is a good opportunity for Congress to show us it can still legislate — and, indeed, Republican Reps. Tim Burchett and Thomas Massie have introduced legislation to regulate plate readers. Among states with rules, the policies vary widely: Utah requires most plate data to be deleted after nine months, New Hampshire after just three minutes. California is weighing a different approach, with no deletion mandate but with a warrant required to search most data older than 75 days. The federal government taking any of these approaches would be better than the status quo.

Flock, clearly feeling the pressure, has thrown privacy advocates a bone by cutting its default storage period from 30 days to seven. But this is not good enough. Our location privacy shouldn't depend upon what one company feels they can get away with before people start sabotaging their technology. We need laws setting retention limits. It is an affront to American ideals of autonomy and civil liberties for law enforcement to amass heaps of location data on people it has no reason to suspect of anything.

If Congress doesn't act, privacy vigilantes will keep sawing down license plate readers — and they'll have some justification to say they had no other option. Congress should prove them wrong.

Catherine Crump is a professor at the University of California law school and director of the Samuelson Law, Technology & Public Policy Clinic.