



Fast-Growing Company Flock is Building a New AI-Driven Mass-Surveillance System

By Jay Stanley
March 03, 2022

A new and rapidly growing surveillance company called Flock Safety is building a form of mass surveillance unlike any seen before in American life. The company has so far focused on selling automatic license plate recognition (ALPR) cameras to homeowner associations and other private parties, as well as to police departments. But it has done so through a business model that effectively enlists its customers into a giant centralized government surveillance network — and the company is aiming to expand its offerings beyond ALPR to traditional video surveillance, while also expanding its AI machine vision capabilities.

In this paper, we look at this company's products, business model, and future aims, and how those embody some of the more worrisome trends in surveillance technology today. Flock is not the only company engaging in mass collection of ALPR data; Motorola Solutions and the company it acquired, Vigilant Solutions, also run a giant nationwide ALPR database, and have recently [made a bid](#) to compete with Flock's strategy. But we focus here on Flock because it is a new, up-and-coming company that industry analysts say is poised for major expansion both geographically and in the kinds of technology it provides.

A public/private license-scanning network

A startup founded in 2017, Flock has grown rapidly, riding two [major trends](#) in the security camera industry: a move to cloud services, and video analytics. The company recently attracted \$300 million in [venture capital investments](#), which industry analysts [say](#) is “unparalleled in the video surveillance industry” and will put the company “in a position to expand aggressively over the next few years.” The company makes grandiose claims about its mission, which it says is to “eliminate nonviolent crime across the United States.”

Flock [says](#) its fixed cameras have been installed in 1,400 cities across the U.S. and [photograph](#) more than a billion vehicles every month, and its [ambition](#) is to expand to “every single city in America.” Flock also provides mobile ALPR devices for police vehicles through a [partnership with](#) the body camera company Axon. Flock’s cameras allow private customers like homeowner associations as well as police customers to create a record of the comings and goings of every vehicle that passes in front of the cameras. But the service goes well beyond that; it feeds that data into a centralized database run by Flock. As the company [tells](#) police:

If you know the specific license plate in question, use FlockOS to get a detailed report of the suspect vehicle’s history over a given timeframe.

Use FlockOS’s local and national search network to find the suspect vehicle across state lines, including up to 1 billion monthly plate reads. All this is included, for FREE, for any Flock Safety customer.

Flock not only allows private camera owners to create their own “hot lists” that will generate alarms when listed plates are spotted, but also runs all plates against state police watchlists and the FBI’s primary criminal database, the National Crime Information Center (NCIC). When a camera scores a hit against one of those databases, law enforcement receives an immediate notification. As Flock CEO Garrett Langley [explained](#) in 2020:

We have a partnership through the FBI that we monitor all of the cameras for about a quarter of a million vehicles that are known wanted — either stolen, it’s a warrant, it’s an amber alert. And so at any given time — about 20 times an hour — we will notify local authorities. ... In January we reported just over 67,000 wanted vehicles across the country.

This giant surveillance network might also be used by immigration authorities to deport people, as is [Motorola’s](#) private ALPR [database](#). [Asked](#) by Vice News whether Flock could be used for such purposes, Langley said, “Yes, if it was legal in a state, we would not be in a position to stop them,” adding, “We give our customers the tools to decide and let them go from there.”

All of this means that those who purchase Flock cameras are effectively buying and installing surveillance devices not just for themselves, but for the authorities as well, adding their cameras to a nationwide network searchable by the police. The closest thing to this model we have seen before is the doorbell camera company Ring, which also raises many [troubling issues](#). But Flock is working (and enlisting its customers to work) directly as an agent of law enforcement even more than Ring. It says it is “working with” over 700 law enforcement agencies and, [according](#) to Langley,

At the end of the day, we view the police department as our actual end-user. They’re the only ones that can make an arrest. So neighborhoods, apartment complexes, motels, hotels, malls, hospitals — they might pay for the camera, but more often than not the only ones that are actually looking at it are the police. ... Most of our software is actually running in the patrol vehicles. So if there’s a crime, or there’s a stolen car that drives by,

we're notifying the nearest officer, typically within a few seconds from when that happens, and they can turn on the blue lights and go get 'em.

As with Ring, police departments appear to be coordinating with Flock in ways that are unseemly for agencies serving the public. Vice [reported](#) that it obtained emails showing that “Flock works closely with police to try and generate positive media coverage, improve their PR strategy, and ... ‘bring more private cameras into the area.’” Flock has also helped write police press releases, Vice found, and officers appear in Flock [promotional videos](#). Emails obtained by the video surveillance industry research group IPVM [show](#) local Texas police referring homeowners associations and other neighborhood groups to Flock, advocating for the company at community meetings, providing the company with neighborhood contact lists, and introducing other police chiefs to company sales managers. In 2020, Langley [told](#) a police audience,

When you partner with Flock ... you're also getting a new ability to do public outreach. ... Every single day we're working with our chiefs and their command staff to host community events, to build awareness, and more importantly, build a common trust and relationship between your constituents and the police department. And the end result is more cameras at no cost to you.

The company has run into [trouble](#) for pushing police departments to embrace its technology without getting the approval of the communities those departments serve. It has also [created conflict](#) in some communities where its cameras have been proposed or adopted, and sparked well-founded concerns that the technology might have a [disproportionate](#) effect on communities of color and other vulnerable communities.

Centralization of data

When a neighborhood association buys a Flock camera, it is basically contributing a piece of equipment to a new nationwide law enforcement surveillance infrastructure that, as Slate [put it](#), means even “small-town police departments can suddenly afford to conduct surveillance at a massive scale.”

Flock can gather the information captured by its cameras around the country into its own centralized database because it is a cloud-based service provider rather than a mere seller of hardware. That database is available to more than [500 U.S. police departments](#). As a business matter, this allows the company to benefit from self-reinforcing [network effects](#). But if Flock cameras become as widespread and densely placed as the company hopes, law enforcement will gain the ability to know the detailed movements of virtually any vehicle for as far into the past as that data is held. That would create enormous risks of privacy violations and other abuses and would have significant legal implications as well.

And the risk of abuse by government is all too real. Unfortunately, this country has a [long tradition](#), extending up to the [present](#), of law enforcement targeting people not because they're suspected of criminal activity but because of their political or religious beliefs or race. That includes quasi-private surveillance. There are also many [documented instances](#) of individual officers abusing police databases, including ALPR databases.

We have long had concerns about the dangers posed by hybrid [public-private surveillance](#) practices — but Flock threatens to take that to a new level. In the past we have [noted](#) that distributed private surveillance cameras are less of a threat to civil liberties than centralized surveillance networks — [but also](#) warned that if all those private cameras were connected to a cloud, the effect would be to re-centralize them. By pulling all the data recorded by its customers — including its police customers — into its own centralized servers, Flock not only creates an enormously powerful private-public machine sweeping up data on Americans’ activities, but puts itself at that machine’s center. It’s bad enough when law enforcement engages in such mass surveillance, but to have such data flowing through a private company creates an additional set of incentives for abuse.

For one thing, there are no checks and balances on the use of this database. The lack of proper checks on the behavior of law enforcement is well established — and studies [suggest](#) improper use of ALPR in particular may be widespread. Nor are there adequate checks on Flock. The company says it only keeps ALPR data for 30 days, but no laws require them to honor that promise. The company controls an enormous data set that could probably be monetized in various ways — and while the company is growing fast now, boom times never last forever. What will future managers do if the company hits tough times, the spotlight has moved on from their controversial role, and they’re tempted to reach for revenue they’re flushing out of their database every 30 days? How might they use their tool against competitors, or against workers, say, if they find themselves fighting a union battle?

We’ve already had a glimpse of what can go wrong with cloud surveillance providers in the case of the company Verkada, which was hacked and found to be [secretly tapping into its customers’ cameras](#). Indeed, think what present or future leaders or employees at Flock could do with that power — or what they could be pressured or forced into doing by unscrupulous government officials. We know that Ring gave workers [access to every Ring camera](#) in the world, together with customer details. Other companies offering cloud services have also run into controversy from granting such access, including [Google](#), [Microsoft](#), [Apple](#), and [Facebook](#). Those companies accessed people’s data to improve their AI models, which are always hungry for real-world data. Flock likewise [says](#) that its cloud architecture “allows us to continue to improve the software and deploy enhancements out to our cameras in real-time.”

Of course, the authorities and the company are not the only possible sources of abuse; there are [plenty of reasons](#) to worry about nosy homeowner association board members and the like using this tool to snoop on the comings and goings of their neighbors (and their neighbors’ friends, family, lovers, etc.). Neighborhood administrators are not subject to even such training and oversight as is applied to the police, and don’t generally know how to impose access restrictions, if they even think of doing so.

It is true that all vehicles are required to display license plates, and in our [past work on ALPRs](#) we have written that license plate readers would pose few civil liberties risks if they only checked plates against legitimate hot lists and these hot lists were implemented soundly. But we also noted that a proliferation of cameras and widespread sharing allow for the creation of intrusive records of our comings and goings, create chilling effects, and open the door to abusive

tracking. And the scale of what Flock is doing goes far beyond what was contemplated when ALPRs first arrived on the scene.

Accuracy problems

ALPR is also bedeviled by accuracy problems. In tests, IPVM [found](#) that Flock's ALPR worked well overall compared to other products — but nothing is perfect, and even a low error rate can produce tragic consequences given the scale of Flock's operations. In particular, IPVM found that Flock's system misidentified a license plate's state about 10 percent of the time. Given that state misidentification errors [have](#) led to innocent people being terrorized by the police as presumed dangerous criminals, that is a real problem.

The FBI's NCIC database that Flock checks plates against is notoriously [inaccurate](#), and people have been [badly harmed](#) by inaccuracies in that database, [including](#) through ALPR cameras. Federal law requires that government agencies maintain records used to make “any determination about any individual” with “such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination.” That doesn't seem like too much to ask — but when it comes to its NCIC database, the FBI felt compelled to [exempt itself](#) from that law.

One detective also [told](#) colleagues [on LinkedIn](#) that “today we almost did a felony stop on a stolen vehicle that wasn't actually stolen,” and reminded them that when dealing with stolen cars they must “remember to remove the vehicle if it's recovered.” A system dependent on busy and sometimes sloppy officers to remember to carry out such follow through is also a recipe for trouble.

Another source of potential error is that Flock's cameras download fresh hit lists from the NCIC only [twice a day](#), which creates the possibility that the removal of a plate from the hotlist will cause out-of-date alerts to be sent to law enforcement for up to 12 hours until the next update.

The accuracy problems with ALPRs have led to [many incidents](#) in which [people](#) have been subject to [traumatic treatment](#) by law enforcement because of errors. And when law enforcement comes running on high alert because technology has raised an alarm, those most likely to be subject to such treatment — or worse — are Black people and members of other vulnerable communities for whom even the most casual encounter with law enforcement can turn deadly.

When the only people running plates were police officers doing so manually and only when they personally witnessed a suspicious vehicle, errors in law enforcement databases like the NCIC occasionally had bad effects. But when plates are being run 500 million times a month, the consequences of errors in those databases become greatly magnified. (For more on the problems ALPR devices present see the ACLU's 2013 [report](#) and this 2017 Electronic Frontier Foundation [page](#) on the technology.)

Beyond license plates

Flock does not plan to remain limited to ALPR cameras. Langley, its CEO, [told](#) IPVM that the company is working on ideas for traditional camera products and sees “a ton of opportunity in the traditional [surveillance] market.”

Already, the photos taken by Flock’s ALPR cameras capture more than just license plates; the photos are used to create what the company [calls](#) a searchable “Vehicle Fingerprint.” Using a “proprietary machine learning algorithm,” the company [says](#), it gathers “vehicle make, type, color, license plate, state of the license plate, covered plates, missing plates, and unique features like roof racks and bumper stickers.” Presumably that would allow searches for all vehicles that include a particular political bumper sticker, enabling people to be targeted based on the exercise of their First Amendment-protected free expression rights.

If Flock applies its public-private business model and its camera technology to ordinary surveillance cameras, it will be super-charging the spread of centralized police camera networks and helping transform video surveillance from sporadic collections of cameras into truly powerful dragnet surveillance tools.

The spread of such systems has been slow because of the expense involved — but Flock could end that. In October 2021, I attended a security conference where security industry analyst and publisher John Honovich of IPVM told attendees that Flock represents a new, disruptive business model in the surveillance video industry. Outdoor cameras have always been orders of magnitude more expensive than indoor cameras, he said, because they are so difficult to install; running power and data lines to outdoor cameras is no easy feat, and they require costly maintenance contracts.

Flock is focused on solving what has been a very hard problem of outdoor installations with a new model based on three technologies that are rapidly improving: solar power, wireless connectivity, and artificial intelligence. The [rapid decline](#) in the cost of solar power has made solar cameras more economical, and wireless connectivity continues to improve as well. Most significantly, perhaps, improving AI computer vision allows cameras to constantly monitor a scene and only send data off the camera when the AI has determined that something of significance has appeared. In the case of ALPR, that would be a vehicle driving by — but it could be anything. Sending still photos or short clips of scenes identified as significant by AI algorithms allows for the installation of large numbers of cameras without the strain on bandwidth and storage capacities that full-motion video cameras often bring.

According to Honovich, “it’s clear that Flock will get much bigger,” and the company is “a threat to any incumbent doing city-wide systems.” One officer says in a company [promotional video](#) that police have even started using the company’s name as a verb — as in, “Have you Flocked that tag yet?”

Expanding analytics

In addition to looking at a move toward full-motion surveillance, Flock's ambitions include expanding its analytics offerings beyond ALPR. Already, for example, its system can carry out what it calls "[convoy analysis](#)," which involves doing proximity analyses to identify vehicles that are near to each other at crucial times and therefore presumably associated with each other. And in a sales video seen by [Vice](#) (apparently since removed from YouTube), the company said it can detect people, cars, animals, and bicycles, a further indication of the company's interest in expanded video analytics.

The company has also announced a troubling expansion of its ALPR devices into audio recording and analytics, [unveiling](#) an augmented version of its ALPR cameras called "Raven" that purports to provide audio gunshot and "crime detection" as cloud services. This service will use AI to attempt to identify the sounds of gunshots, screeching tires, breaking glass, and sawing metal (to try to detect catalytic converter theft).

The Raven product raises questions about Flock's direction as AI and machine vision continue to improve. Today the company reads license plates and bumper stickers; tomorrow that could expand to t-shirts and tattoos. And how long before it offers products claiming to be able to visually detect guns, fighting, muggings, "[aggression](#)," or "anomalous" behavior? All of these and many more capabilities are currently being worked on by computer scientists. We discussed this trend in more detail in our 2019 [report](#) on video analytics, but the long-term threat is that millions of cameras will be turned into ever-watchful digital officers, never sleeping or distracted but highly biased and error-prone, monitoring us constantly and ready to report us to our neighbors or the authorities. Indeed, one of Flock's [marketing slogans](#) makes this analogy explicit, saying that its cameras "see like a detective."

Flock has another product called "[Wing](#)" that allows police to scan through thousands of hours of footage to extract vehicle "fingerprints" for searching — an extremely powerful new surveillance capability. It can thus transform existing third-party cameras owned by police departments into cameras that the company says can — yes — "see like a detective." The power of cloud AI analytics is that they're not tied to any particular hardware.

Even more so than license plate recognition, other forms of AI are also notoriously [brittle](#) and unreliable. It's highly questionable how effective Flock's Raven audio analytics service will be, for example. The gunshot detection company ShotSpotter similarly [uses](#) microphones distributed across a city to listen for gunshots, but mostly relies on human analysts to try to differentiate between gunshots and other loud bangs — and even so, questions have been [raised](#) about ShotSpotter's false alarm rate and overall effectiveness. The number of false alarms triggered by Raven will likely prove to be significant and perhaps dysfunctional.

And of course, Flock will want to access its customers' cloud data in order to improve its AI, as it says it is already doing with ALPR data. If and when the company moves into collecting live video and other increasingly sensitive data, it will create a significant privacy issue as well. Raven also raises significant legal issues due to wiretapping laws (see below).

Flock is already building an unprecedented, public-private, distributed-yet-centralized surveillance machine. All the risks posed by such a machine will only grow if the company

expands its offerings from ALPR to traditional surveillance cameras and to advanced new forms of behavioral analytics.

Privacy practices

Flock constantly [claims](#) to be “privacy friendly” to try to disarm one of the primary obstacles to its acceptance by communities. It says it doesn’t do face recognition, which is good (though that wouldn’t stop an end-user police department from doing so once it had downloaded an image of a person). For auditing purposes, it includes a data field in which police enter the reason for a search, which is good. It also says it doesn’t sell or share ALPR data with third parties (other than through its database service, which is part of what it is selling with its products), and only retains plate data for 30 days. “With built-in 30-day data retention, everyone’s comfortable,” Langley [claims](#).

Everyone is not comfortable. An even shorter retention period would be better, but this system would be far worse than it is if the retention period were longer. Still, given the scale of this system, 30 days is a long enough window that it poses real privacy risks, especially if Flock cameras continue to grow, providing an ever-more-detailed record of people’s movements. People can engage in a lot of perfectly legal yet private behavior within 30 days — movements that would reveal things about their political, financial, sexual, religious, or medical lives that nobody in the police or in a company like Flock has a right to track. As discussed below, a majority on the Supreme Court has [explained](#) that tracking a vehicle with GPS constitutes a “search” for Fourth Amendment purposes even when the tracking only lasts 28 days. And the court later held that obtaining seven days of location information about a person was a Fourth Amendment “search,” too.

Whenever questioned about privacy, Flock executives mention these policies, as if that’s the end of it. But it’s not the end of it; there are many other privacy implications of license plate recognition in general, and Flock’s system in particular, that communities need to consider. Flock may not sell its data but the company itself holds it. And as IPVM aptly [put it](#), if the company achieves its growth targets, “it will effectively become a gigantic private entity that is performing public policing work.” The privacy protections Flock likes to tout are necessary but not sufficient in a system playing that role at such a scale, and Flock’s products raise many privacy issues that aren’t addressed by the privacy practices that they cite. And again, we have no way of knowing whether Flock is following its stated policies, and it could change those policies at any time.

A system of mass surveillance

Altogether, Flock’s ALPR network adds up to a system of mass surveillance — a system that seems poised to expand beyond just license plate recognition. Mass surveillance systems have long been feared by people who value open, democratic societies, and for good reason. The ability to access a record of all our activities — even if just when we’re in public spaces — conveys the power to learn an enormous amount about our social, political, sexual, medical, and religious lives. Mass surveillance simply gives too much power to those who control it. Such

power lends itself too easily to abuse, chilling people who might want to protest those in power or otherwise exercise their freedom of expression, and generally casting a pall over people's freedom to live their lives without being watched.

Surveillance systems also tend to have a disproportionate impact on Black and Brown and other historically disadvantaged communities. Often police departments [install them disproportionately](#) in communities of color. The NYPD [used](#) ALPR devices to abusively [surveil mosques](#) in the 2000s. And systems such as Flock's enable the continuation and intensification of patterns of policing such as those uncovered by the Department of Justice in Ferguson, Mo. There, the DOJ found in a [comprehensive report](#) that the police department aggressively over-enforced low-level, nonviolent "offenses" in communities of color (a [pattern](#) that has been found across the nation, including in [New York City](#), [Minneapolis](#), [Chicago](#), [North Carolina](#), [Philadelphia](#), and [Boston](#)). In Ferguson and some other jurisdictions, low-level arrests were intentionally used to extract payments to fill municipal coffers. This practice draws poor people who can't pay fines or who miss court dates into an escalating cycle of fees, fines, police stops, and general entanglement with the criminal justice system, amplifying petty offenses into ruined lives in a truly Dickensian dynamic. Many of those stops and fines involve automobiles, and a dragnet ALPR surveillance system [lends itself very naturally](#) to supporting that kind of policing.

Legal analysis

The system that Flock has built and is building could have many bad effects, but does it violate the law or Constitution?

The first question is whether the fact that people and/or their license plates are being photographed in public means that there can't be any legal violation of privacy. That claim does not appear to be winning acceptance in the courts.

In a pair of cases involving police use of digital-age technologies to track or aggregate peoples' locations and movements, the Supreme Court has [explained](#) that "individuals have a reasonable expectation of privacy in the whole of their physical movements" because of the "privacies of life" those movements can reveal. In *United States v. Jones*, a majority of the court wrote that using a GPS tracker to follow a car's movements for 28 days constitutes a Fourth Amendment search, observing that the ability to "secretly monitor and catalogue every single movement of an individual's car for a very long period" raised serious concerns. More recently, the court held in *Carpenter v. United States* that when police request seven days or more of a person's historical cell phone location information from a cellular service provider, a warrant is required. That's because of the "deeply revealing nature" of these digital location records, their "depth, breadth, and comprehensive reach," and the "inescapable and automatic nature of [their] collection." These rulings expressly rejected the argument that the public nature of the targets' movements meant they had no legally significant expectation of privacy.

Automated license plate readers raise the same concerns the court addressed in *Jones* and *Carpenter*: they facilitate detailed, pervasive, cheap, and efficient tracking of millions of Americans in previously unthinkable ways. ALPR data can reveal private and sensitive details about a person's life — details that individuals reasonably expect to remain private — and

searches of ALPR databases by law enforcement to find evidence of criminal activity should require a warrant. As the Massachusetts Supreme Judicial Court [recently observed](#), “With enough cameras in enough locations, the historic location data from an ALPR system ... would invade a reasonable expectation of privacy and would constitute a search for constitutional purposes.”

And what holds for ALPR cameras should also hold for any future mass-surveillance camera systems that can track people in equivalent ways — for example, by using a centralized network of public and private cameras combined with face recognition or other forms of video analytics or biometrics.

The second question is whether Flock’s status as a private company affects this analysis — after all, only the government is constrained by the Fourth Amendment. And in fact, in many contexts, private actors have a right to take photographs that is *protected* by the Constitution’s First Amendment. That right is not absolute, however; lawmakers, if they so choose, do have the authority to regulate photography that interferes with Americans’ reasonable expectations of privacy, such as in private spaces like restrooms or people’s homes. The deployment by private parties of surveillance systems such as camera networks that track people across space and time implicate similarly pressing privacy concerns.

But if lawmakers fail to enact such privacy protections, does the Constitution have anything to say about a private company like Flock engaging in such surveillance? It might, if Flock were acting in concert with police departments to the extent that courts would consider it a “[state actor](#).” In past cases, the Supreme Court has found private parties to be state actors (and therefore subject to the Constitution and other laws that apply to the government) where:

- Private parties perform public functions that have traditionally and exclusively been performed by the government.
- The government influences and encourages the performance of private actions.
- The government and a private actor enter into a “joint enterprise” or “symbiotic relationship” or become “pervasively entwined” with each other.

This body of law prevents the government from evading its constitutional responsibilities by delegating power to and hiding behind private entities. In the ACLU’s recent [successful challenge](#) to the City of Baltimore’s persistent aerial surveillance program, the City did not even dispute that the third party surveillance vendor conducting its surveillance operations was a state actor under the relevant law. Given Flock’s actual entanglement and symbiotic relationship with law enforcement, there would at a minimum be a plausible case that Flock fits this definition and that its ALPR services — and potentially other mass-surveillance services such as a Raven audio recording network or other future offerings — are therefore constrained by constitutional privacy rights.

State laws are also relevant in assessing the legality of ALPR deployments. [Sixteen states](#) have passed statutes regulating ALPR devices. A few state laws regulate or ban certain private uses of ALPR, which would of course directly affect the legality of Flock’s business model in those states. But most of the state laws regulate how law enforcement uses ALPR. California, for

example, bans state police departments from sharing ALPR data with out-of-state and federal agencies, but a number of departments are [violating the law](#). (The ACLU of Northern California is [suing](#) over this violation.)

State constitutions, many of which have stronger privacy protections than the federal Constitution, may also impose limits on private surveillance business models such as Flock's. Some state constitutions, such as [California's](#), also place more limits on private actors.

A major question this raises is whether any police departments are using their reliance on this private company to do an end run around these laws. [Judges](#) in Virginia, for example, [ruled](#) that a Virginia privacy law (which says that personal information “shall not be collected” by state agencies “unless the need for it has been clearly established in advance”) bars police from collecting and storing ALPR data outside of a specific investigation. But if the State Police were accessing Flock's ALPR database without considering themselves as “collecting” the data held by Flock, that would represent an evasive end-run around the intent of Virginia's law.

Raven

Aside from threatening to expand daily surveillance in American life [from video to audio monitoring](#), Flock's Raven gunshot detection product also raises significant legal questions. While the United States has millions of video cameras in public places, very few of them include microphones, and there's a good reason for that. It's not because mics are expensive or difficult to install, but because our wiretapping laws make it legally problematic to audio record people in public places. Laws in all the states and federal law make it illegal to record a conversation where the recording party is not a participant — and some state laws require the permission of all participants in a conversation. ShotSpotter's microphones have survived scrutiny on this score partly because most of its mics are placed high above street level, where they can better hear gunshots and be shielded from everyday sounds. Those mics are also very narrowly targeted toward listening for gunshots, and there is no important privacy interest when it comes to the sound of gunshots in a city. Even so, we and other privacy advocates have been [very wary](#) about ShotSpotter's product on that score.

But Flock's audio sensors, which come packaged with the license plate readers, are placed close to the ground so the ALPR can see vehicles, and are therefore much more likely to pick up conversations. They also extend their monitoring beyond loud percussive noises to other noises that are much more likely to be a regular part of human life. By listening for a broader variety of more ambiguous sounds, Raven is more likely to accidentally record conversations. And in the rich and complicated lives we lead, people might have good reasons to break glass, or saw metal, or make screeching sounds — not to mention other noises that might be mistaken for those sounds by the AI — and shouldn't have to worry about police arriving on the scene every time they do so.

Just recently my neighbor was bringing home groceries and dropped and shattered a glass bottle in her driveway. I found myself thinking about Flock's product and how glad I was she didn't have to worry about the police showing up — something that, again, poses particular dangers for people of color.

Recommendations for Public-Private Surveillance Systems

Our nation should not permit the construction of any mass-surveillance systems, including through private-public law enforcement systems such as that being built by Flock. Legislators should enact rules governing ALPR along the lines of the [recommendations](#) we laid out in our 2013 report, and extend them to private actors working closely with law enforcement. Policymakers should include the following updates to account for the changing landscape:

- Given the increasing regional and national reach of ALPR systems, any non-hit data they collect should be permitted to be held only for very short periods. New Hampshire [state law](#) is a good model; it requires that where there is a hit, ALPR data “shall not be recorded or transmitted anywhere and shall be purged from the system within 3 minutes of their capture.” That policy allows the devices to be used to search for wanted vehicles but prevents the creation of dragnet location tracking databases. Retention periods of 30 days are too long for surveillance systems with a breadth and scope of any significance.
- No hot lists should be used unless they are certified by independent auditors as meeting the highest standards of due process (allowing people a meaningful way to have themselves or their vehicles removed including through adjudication by a neutral arbiter), legitimacy (being based only on individualized suspicion, and not being based on First Amendment-protected activity, for example), and reliability (including those standards imposed by the Privacy Act of 1974, a standard that the NCIC does not currently meet).
- Law enforcement agencies should not share license plate reader data with third parties that do not conform to the above principles and should be transparent regarding with whom license plate reader data is shared.
- Communities and their elected representatives should be especially hesitant to embrace networked surveillance cameras. Before investing in a partnership with Flock they should do some very careful legal analysis in light of the Supreme Court’s *Carpenter* decision.
- Communities that have not yet enacted a Community Control Over Police Surveillance (CCOPS) ordinance should not permit the police that serve them to deploy surveillance devices without first receiving approval from the city council or other elected governing body. The decision-making process around whether to deploy surveillance technology should be transparent and open to public input and debate.

Businesses, community associations, and other private parties should consider the following when evaluating or deploying this technology:

- Private institutions should, at a minimum, think long and hard about whether they truly need ALPR or other dragnet surveillance devices, especially where vendors allow law enforcement — local and not — to search the data collected by any such devices.

- Private institutions should not use ALPR or other dragnet surveillance devices unless they disclose that fact to their customers, residents, or others subject to the surveillance.
- Housing and community associations that adopt such systems should ask sharp questions about their deployment such as: Who will have access to the data that is collected about you, your family, and friends or other visitors? Will there be any restrictions on the purposes for which data is accessed, or with whom it is shared, or can those with access browse through the data whenever they want? How will requests for access by residents, non-residents, those accused of wrongdoing, media outlets, or others be handled? Is there any logging of access to the data, or other mechanisms for enforcing rules about sharing and access?
- Any associations that create their own hotlists should do so only in conformance with the principles above that are applicable to government hot lists. They should also create and publish policies people driving throughout the community can read and understand.

Conclusion

Flock is pushing the adoption of surveillance devices by private parties and folding them into a larger, centralized network that is fast becoming a key policing infrastructure, all while pushing to expand beyond license plate recognition to other forms of AI machine vision and simultaneously making it much easier to install and connect outdoor cameras. If successful, the convergence of these trends — whether under the aegis of Flock or other companies — threatens to bring an entirely new level of surveillance to American communities, where it will further undermine Americans' privacy, disproportionately harm historically disadvantaged communities, and generally shift power to the government from the governed in our nation.

###