



CITY OF CARMEL-BY-THE-SEA Notice and Agenda

Contact: 831.620.2000 www.ci.carmel.ca.us

Community Meeting Notice

Thursday, October 24, 2024
1:00 PM

FLOCK CAMERA AD HOC COMMITTEE MEETING

WHAT: Community meeting hosted by Councilmember Alissandra Dramov and Mayor Pro Tem Bobby Richards with staff support from Chief Tomasi, to discuss and receive feedback from the public on the number and location of the Flock license plate reader cameras throughout the Village. Information gathered from the meeting will inform a future Ad Hoc Committee recommendation to the full City Council.

WHERE: City Council Chambers located on Monte Verde Street between Ocean and Seventh Avenues, Carmel-by-the-Sea, and via Zoom Webinar.

ATTENDANCE OPTIONS: The meeting will be held in person in the Council Chambers and via Zoom Webinar. You may also watch the livestream on the City's YouTube Page at: <https://www.youtube.com/@CityofCarmelbytheSea/streams>. Please note that the community meeting will proceed as normal even if there are technical difficulties accessing Zoom. The City will do its best to resolve any technical issues as quickly as possible. To participate in the meeting via Zoom, copy and paste the link below into your browser.

<https://ci-carmel-ca-us.zoom.us/j/83037519057> Webinar ID: Webinar ID: 830 3751 9057
Passcode: 278872 Dial in: (253) 215-8782

HOW TO PARTICIPATE: The public may give their comments on Flock Cameras in person, or using the Zoom teleconference module, provided that there is access to Zoom during the meeting. Zoom comments will be taken after the in-person comments. The public can also email comments to cityclerk@ci.carmel.ca.us, with "Flock Cameras" in the subject line of the email. Speakers will have five (5) minutes to speak; but that limit may be increased or decreased at the meeting.

AGENDA ITEMS:

- A. Introduction and Welcome from the Flock Camera Ad Hoc Members, Councilmember Dramov and Mayor Pro Tem Richards
- B. Discussion and information gathering session on the number and placement of Flock license plate reader cameras throughout the Village.

ADJOURNMENT

- A.** Correspondence Received After Agenda Posting
- B.** Presentation and other documents received after agenda posting

This agenda was posted at City Hall, Monte Verde Street between Ocean Avenue and 7th Avenue, Harrison Memorial Library, located on the NE corner of Ocean Avenue and Lincoln Street, the Carmel-by-the-Sea Post Office, 5th Avenue between Dolores Street and San Carlos Street, and the City's webpage <http://www.ci.carmel.ca.us> in accordance with applicable legal requirements.

SPECIAL NOTICES TO PUBLIC

In compliance with the Americans with Disabilities Act, if you need special assistance to participate in this meeting, please contact the City Clerk's Office at 831-620-2000 at least 48 hours prior to the meeting to ensure that reasonable arrangements can be made to provide accessibility to the meeting (28CFR 35.102-35.104 ADA Title II).



CITY OF CARMEL-BY-THE-SEA COMMUNITY MEETING Staff Report

October 24, 2024

TO:	Community Meeting Members
SUBMITTED BY:	Chip Rerig, City Administrator
SUBJECT:	Discussion and information gathering session on the number and placement of Flock license plate reader cameras throughout the Village.

RECOMMENDATION:

Hold a discussion and information gathering session on the number and placement of Flock license plate reader cameras throughout the Village.

BACKGROUND/SUMMARY:

On June 10, 2024, the Flock Ad Hoc Committee held a Community Meeting to discuss the Flock Cameras and answer questions from the public. Staff's presentation slides from the June 10, 2024 Flock Ad Hoc meeting are attached to this staff report as **Attachment 1** for additional background.

FISCAL IMPACT:

PRIOR CITY COUNCIL ACTION:

ATTACHMENTS:

Flock Camera Presentation - 6-10-2024 Ad Hoc Meeting

flock safety



Ad Hoc Committee Meeting

June 10th 2024



Today's Topics

- Introduction to Flock
- Addressing Community Concerns
 - Privacy
 - Number of Cameras
 - Location of Cameras
 - Aesthetics

What is Flock?

- Founded in 2017
- License Plate Reader (LPR) Technology
- Used in 42 US States and 4,000+ cities;



Monterey County Agencies Using Flock

- Pacific Grove PD - 12
- Salinas PD - 72
- Marina - 20
- Seaside - 25 + 1 mile gunshot detection
- Sand City - 10
- Monterey - 34
- Soledad- 6 (final council approval next week)
- Monterey Co - 60




How Flock Works?

- Photographs license plates and stores that image in the cloud
- Sends a notification to email or phone if a:
 - Stolen vehicle is detected
 - Stolen license plate is detected
 - Amber or Silver alert (Missing children/adults)
 - Manuel entry for wanted person or vehicle

What happens when a wanted vehicle passes a FLOCK camera?

A text message or email is sent to the police officers on duty, notifying them of a stolen vehicle/wanted vehicle/missing person. A photograph is also sent

Plate	→ CA 7EMS6	Source	California SVS	Camera	#13 Leavesley Rd @
Date	5/14/2024, 11:34:23 AM 3 hours ago	Topic	Stolen Vehicle	Network	101 Off Ramp - WB Gilroy CA PD

		
--	---	--

Recent Carmel Police Department Flock Alerts:

04/30/2024: A person wanted for sexual assaulting a 7 year old in Seaside was captured on Flock. The suspect was arrested.

1 Objects

100







Plate CA 9EZC

Date 4/29/2024, 11:30:36 AM

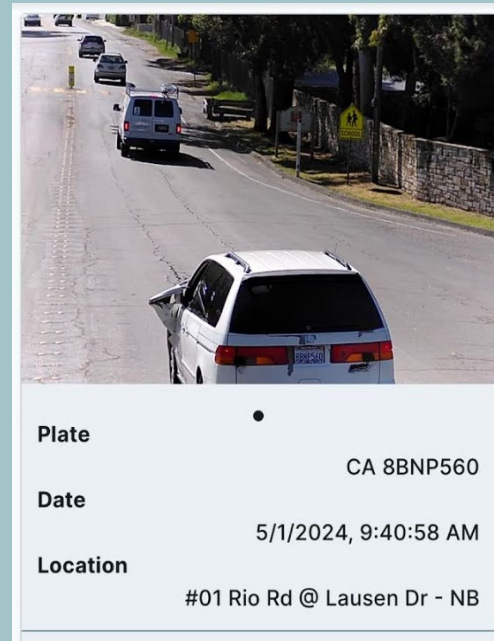
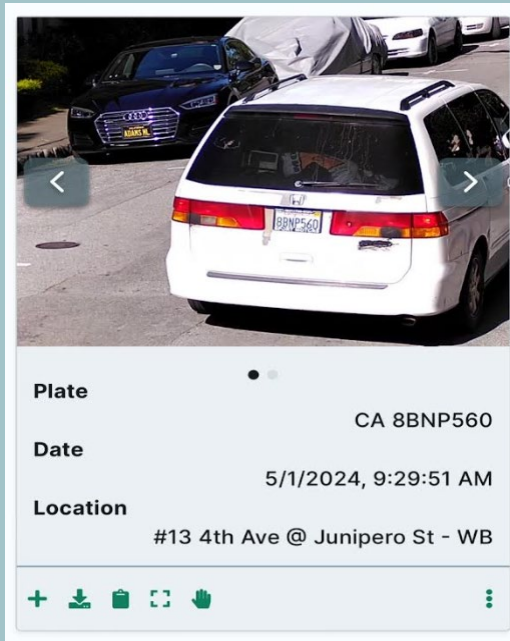
Location #18 Monte verde St @ 6th Ave - SB

Plate	List Name	Camera
CA 9EZCS	Suspicious vehicle	#06 Ocean Ave @ Junipero St - EB
Date	Case Number	Network
4/30/2024, 3:02:42 PM	Seaside 288 Seaside	Carmel CA PD

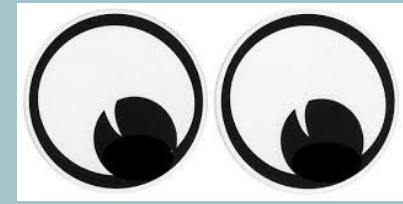


Recent Carmel Police Department Flock Alerts:

On 5/1/24, Seaside and Monterey Police were searching for a carjacker, burglar, and kidnapper, last seen driving a white van with license plate 8BNP560



Privacy Concerns



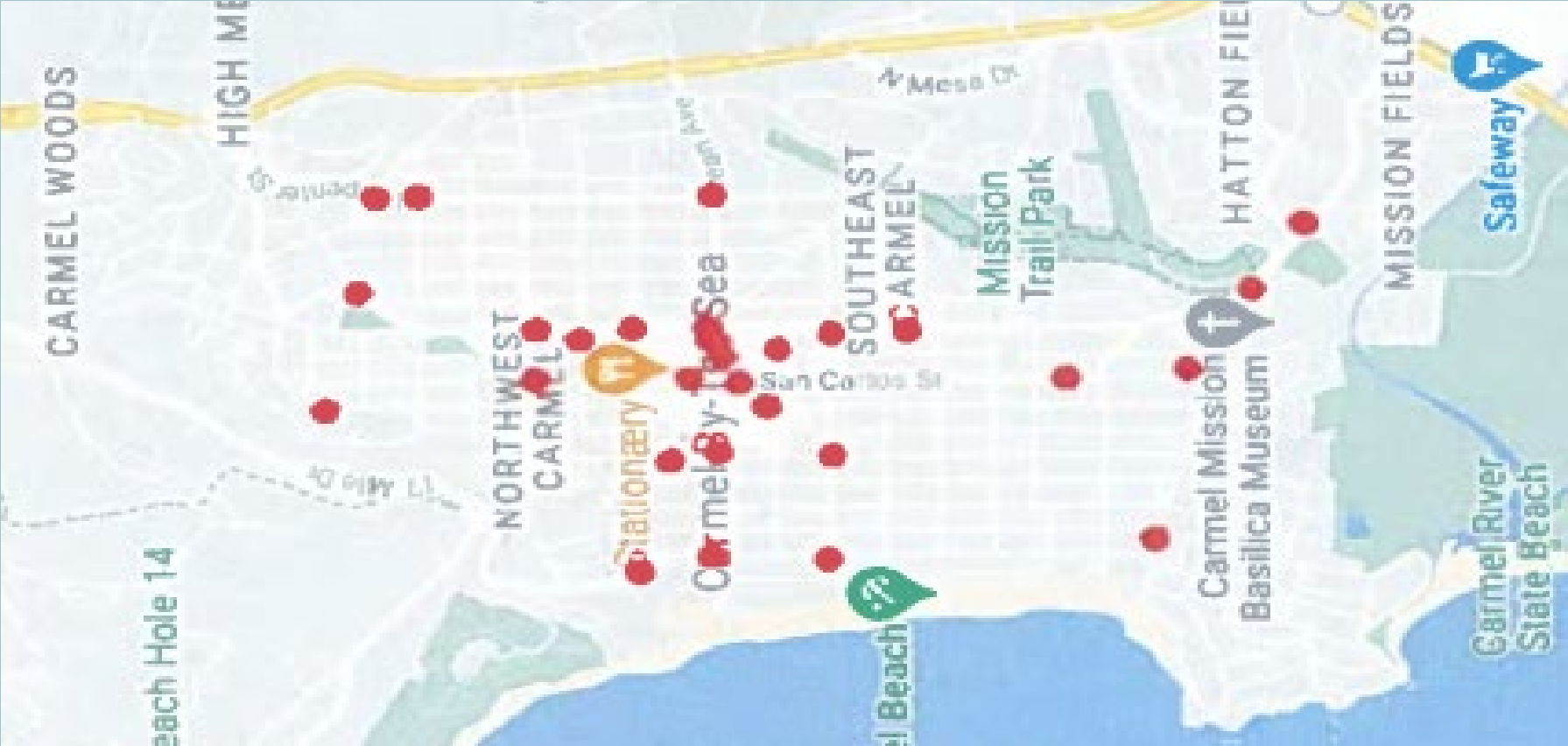
- Flock does **not** capture people (i.e Facial recognition)
- Data is only retained for 30 days
- Manual searches for license plates can be done but only with a report number or reported crime (Misdemeanor or Felony)
- Flock does not continuously record or record live feeds
 - We do have 6 perimeter cameras that do live feed (approved by council in 2017)



Transparency Portal

- ci.carmel.ca.us/police-fire
- External organizations share
- Number of searches in last 30 days (29 as of 5/14/24)
- Public Search Audit (Date, time, reason why the search was done)

Camera Locations in CBTs



Number of Cameras

What's the Right Number?

Valuable tool for Police

- Crime Trends
 - Robbery/Theft Crews
 - Sideshow Activity
- Missing Persons
- Stolen Vehicles



BURGLARIES



CARMEL POLICE OUT NUMBERED BY CRAZY SUPERCARS STUNTING!!

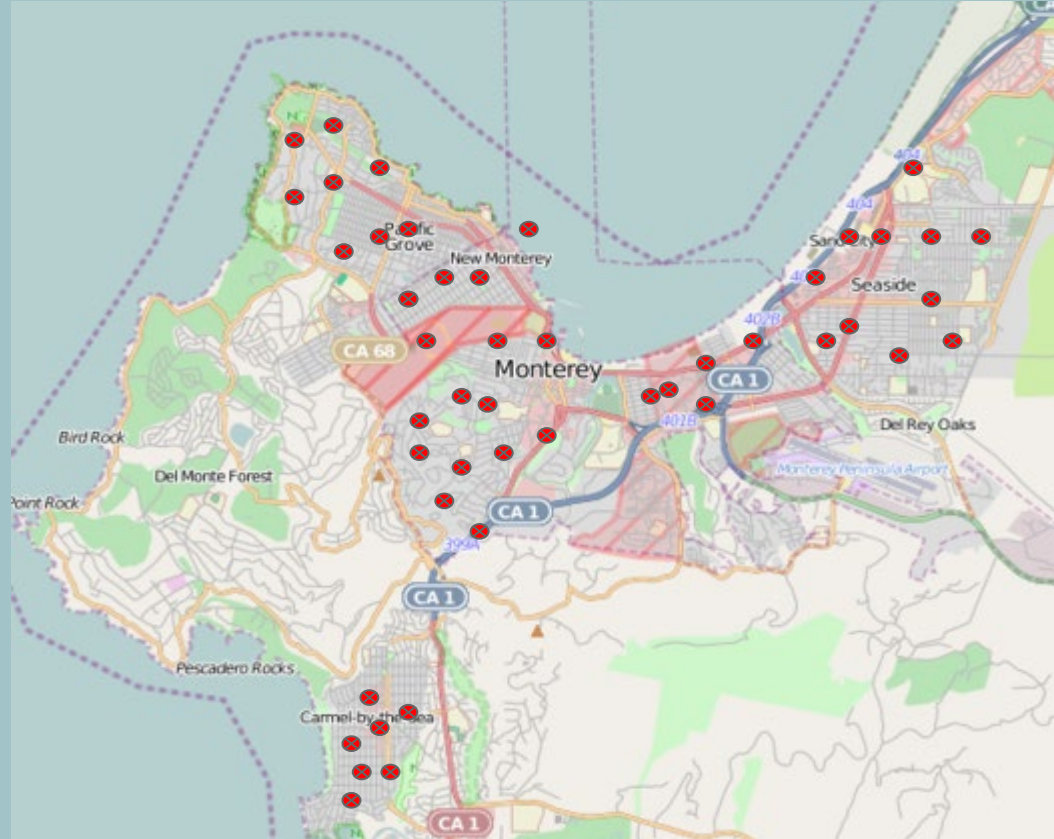


Number of Cameras

- Crime Fighting Techniques
 - 2000 era – ROPE – Roadblock Observation Plan or Enforcement
 - Flock helps us prevent crime and Catch Criminals
- Change in Policing
 - Techniques
 - Staffing

Network of Cameras

- Using Technology to our Advantage



Number of Cameras

What is a good Balance?

Goal

- Keep Community Safe
- Prevent Crime
- Solve Crimes
- Business District Only?
- Residential District Only?
- Combination?



Aesthetics

What do we want?

- Solar?
- Electric?
- Combination? (Electric where possible?)



Goal: Place cameras in the most beneficial locations while not disrupting the look of the village.

Questions

?

Recommendation

Chief's Recommendation!!!

1. Begin w/Flock Cameras at Perimeter Camera Locations (6)- Outer Perimeter
2. Add Cameras around Business District (10-17)-Inner Perimeter-No cameras in residential area (except for (6) on Perimeter Cameras
3. Look for hardwiring options in as many locations as possible- Light Poles, PG&E poles, Eaves of businesses. Solar only in areas where no other option is available.
4. Provide yearly report to council on camera use. (Justify Numbers) Council to approve contract extension & number of cameras.

Next Steps

- Identify locations in business district where cameras can remain, be installed, be removed. Come back in July with specific locations and numbers of cameras in downtown between 10-20.



CITY OF CARMEL-BY-THE-SEA COMMUNITY MEETING Staff Report

October 24, 2024

TO: Community Meeting Members
SUBMITTED BY: Chip Rerig, City Administrator
SUBJECT: Correspondence Received After Agenda Posting

RECOMMENDATION:

BACKGROUND/SUMMARY:

FISCAL IMPACT:

PRIOR CITY COUNCIL ACTION:

ATTACHMENTS:

Correspondence #1



Nova Romero <nromero@ci.carmel.ca.us>

Ad hoc Flock cameras 🙄 must read

christy Hollenbeck [REDACTED] >

Wed, Oct 23, 2024 at 11:57 PM

To: Bobby Richards <brichards@ci.carmel.ca.us>, Alissandra Dramov City 📍 <adramov@ci.carmel.ca.us>, Nova Romero <nromero@ci.carmel.ca.us>, Mayor Dave Potter <dpotter@ci.carmel.ca.us>, Karen Ferlito <kferlito@ci.carmel.ca.us>, Jeff Baron <jbaron@ci.carmel.ca.us>

**Please enter into the record for the Flock Camera Ad Hoc meeting.
Thank you!
Christy Hollenbeck**

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

By Jay Stanley
March 3, 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.

Sent from my iPad

2 attachments



IMG_1020.png
389K

flock_1.pdf
327K



RECOMMENDATIONS

To ensure that license plate readers can be used by law enforcement agents for legitimate purposes without infringing on Americans' privacy and other civil liberties, the ACLU calls for the adoption of legislation and law enforcement agency policies adhering to the following principles:

- License plate readers may be used by law enforcement agencies only to investigate hits and in other circumstances in which law enforcement agents reasonably believe that the plate data are relevant to an ongoing criminal investigation. The police must have reasonable suspicion that a crime has occurred before examining collected license plate reader data; they must not examine license plate reader data in order to *generate* reasonable suspicion.
- Law enforcement agencies must not store data about innocent people for any lengthy period. Unless plate data has been flagged, retention periods should be measured in days or weeks, not months, and certainly not years.
- It is legitimate to flag plate data (1) whenever a plate generates a hit that is confirmed by an agent and is being investigated, (2) in other circumstances in which law enforcement agents reasonably believe that the plate data are relevant to a specific criminal investigation or adjudication, (3) when preservation is requested by the registered vehicle owner, or (4) when preservation is requested for criminal defense purposes.
- Once plate data has been flagged, a longer retention period commensurate with the reason for flagging is appropriate.
- Law enforcement agencies must place access controls on license plate reader databases. Only agents who have been trained in the departments' policies governing such databases should be permitted access, and departments should log access records pertaining to the databases.
- People should be able to find out if plate data of vehicles registered to them are contained in a law enforcement agency's database. They should also be able to access the data. This policy should also apply to disclosure to a third party if the registered vehicle owner consents, or for criminal defendants seeking relevant evidence.
- Law enforcement agencies should not share license plate reader data with third parties that do not conform to the above retention and access principles, and should be transparent regarding with whom license plate reader data are shared.

Attachment 1



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

By Jay Stanley
March 3, 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 has a [partnership with](#) the body camera company Axon to provide mobile ALPR devices for police vehicles. 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 [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.

###



**Carmel-
by-the-Sea**

Nova Romero <nromero@ci.carmel.ca.us>

Oakland CA Prvacy advisory commission ordinance.

christy Hollenbeck <[REDACTED]>

Wed, Oct 23, 2024 at 9:14 PM

To: Nova Romero <nromero@ci.carmel.ca.us>, Bobby Richards <brichards@ci.carmel.ca.us>, Alissandra Dramov City <adramov@ci.carmel.ca.us>

Please enter into the record for Flock Camera AD Hoc meeting. Thank you!

Christy Hollenbeck

<https://cao-94612.s3.us-west-2.amazonaws.com/documents/OMC-9.64-January-2021-005.pdf>

Privacy Advisory Commission

The Privacy Advisory Commission provides advice to the City of Oakland on best practices to protect Oaklanders' privacy rights in connection with the City's purchase and use of surveillance equipment and other technology that collects or stores our data.

<https://cao-94612.s3.us-west-2.amazonaws.com/documents/OMC-9.64-January-2021-005.pdf>

Sent from my iPad

3 attachments

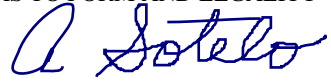


logo-oakland.png
57K

 **OMC-9.64-January-2021-005.pdf**
188K

 **OMC-9.64-January-2021-005.pdf**
188K

APPROVED AS TO FORM AND LEGALITY



CITY ATTORNEY'S OFFICE

OAKLAND CITY COUNCIL

ORDINANCE NO. _____ C.M.S.

ORDINANCE AMENDING OAKLAND MUNICIPAL CODE CHAPTER 9.64, WHICH REGULATES THE CITY'S ACQUISITION AND USE OF SURVEILLANCE TECHNOLOGY, BY (A):

- (1) CLARIFYING EXISTING DEFINITIONS AND ADDING NEW ONES;**
 - (2) CLARIFYING WHEN CITY STAFF MUST NOTIFY THE PRIVACY ADVISORY COMMISSION AND/OR SEEK CITY COUNCIL APPROVAL IN REGARDS TO THE ACQUISITION OF SURVEILLANCE TECHNOLOGY;**
 - (3) PROHIBITING THE CITY'S USE OF BIOMETRIC SURVEILLANCE TECHNOLOGY AND PREDICTIVE POLICING TECHNOLOGY;**
- AND**
- (B) ADOPTING CALIFORNIA ENVIRONMENTAL QUALITY ACT EXEMPTION FINDINGS**

WHEREAS, the City of Oakland first adopted a Surveillance Technology Ordinance (codified as Oakland Municipal Code or O.M.C. Chapter 9.64) in May 2018 and City staff have been working closely with the Privacy Advisory Commission (PAC) and learning from the implementation process since that time, and have identified areas that require refinement and/or clarification; and

WHEREAS, the PAC has recommended that the definition of the Annual Surveillance Report should be revised to include information regarding the reporting of data sharing with outside entities, and information on the race of individuals that may have been identified using surveillance technology; and

WHEREAS, the use of Biometric Surveillance Technology by government agencies in real time or on a recording or photograph is a growing concern for civil liberties and privacy advocacy groups; and

WHEREAS the United States Department of Defense announced in June 2020 it was testing a new laser-based Biometric Surveillance Technology system capable of identifying people at a distance of up to 200 meters by measuring their heartbeat, and police in China are testing gait-recognition Biometric Surveillance Technology that identifies people based on how they walk; and

WHEREAS, the proposed amendments to O.M.C. Chapter 9.64 include a definition of the term Biometric Surveillance Technology and a provision banning the City's use of such technology; and

WHEREAS, there are other forms of Surveillance Technology that use biometric information, where such information is not collected in real time. Such technology is vital to traditional operations of the City's Police Department Crime Laboratory for solving serious violent crimes and needs to be distinguished from what this ordinance defines as Biometric Surveillance Technology; and

WHEREAS, Predictive Policing Technology uses arrest data that can encode patterns of racist policing behavior and as a result, are more likely to predict a high potential for crime in minority neighborhoods or among minority people and several studies have shown that these tools perpetuate systemic racism, leading to disparate arrest rates; and

WHEREAS, traditional records management systems, including computer aided dispatch systems, and field-based reporting systems, and Live Scan Machines do not pose significant civil liberty risks and should not be regulated in the same manner since they serve a critical core function of the police department; and

WHEREAS, it is important that City departments seek approval from the City Council prior to purchasing or using new surveillance technology but should not have to return repeatedly for technology that already has an approved Use Policy in place; and

WHEREAS, the Privacy Advisory Commission met with City staff on several occasions to refine the current ordinance to better protect Oaklander's Civil Liberties and improve upon the original reporting and approval processes; and

WHEREAS, the City Council has determined that this action is exempt from environmental review under the California Environmental Quality Act (CEQA) pursuant to: (1) CEQA Guidelines Section 15061(b)(3), Review for Exemptions – General Rule, in that it can be seen with certainty that there is no possibility for this action to have a significant effect on the environment; and (2) CEQA Guidelines Section 15378(b)(5), since this action does not constitute a “project” within the meaning of CEQA and instead relates to “[o]rganizational or

administrative activities of [the City] that will not result in direct or indirect physical changes in the environment.”

NOW, THEREFORE, THE CITY COUNCIL OF THE CITY OF OAKLAND DOES ORDAIN AS FOLLOWS:

SECTION 1. Recitals. The City Council finds and determines the foregoing recitals to be true and correct and hereby adopts and incorporates them into this Ordinance.

SECTION 2. Amendments to Chapter 9.64 of the Oakland Municipal Code. Oakland Municipal Code Chapter 9.64, is hereby amended as set forth below. Chapter and section numbers and titles are indicated in bold type. Additions are indicated in underline and deletions are shown as ~~strikethrough~~. Provisions of Chapter 9.64 not included herein or not shown in underline or strikethrough type are unchanged.

9.64.010 - Definitions.

The following definitions apply to this Chapter.

1. "Annual Surveillance Report" means a written report concerning a specific surveillance technology that includes all the following:
 - A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology;
 - B. Whether and how often data acquired through the use of the surveillance technology was directly shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);
 - C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to;
 - D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year;
 - E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties.

The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review;

- F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information;
 - G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response;
 - H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes;
 - I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates;
 - J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year; and
 - K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request.
2. "Biometric Surveillance Technology" means any computer software that uses Face Recognition Technology or Other Remote Biometric Recognition in real time or on a recording or photograph.
- ~~2~~3. "City" means any department, agency, bureau, and/or subordinate division of the City of Oakland as provided by Chapter 2.29 of the Oakland Municipal Code.
- ~~3~~ 4. "City Staff" means City personnel authorized by the City Administrator or designee to seek City Council approval of surveillance technology in conformance with this Chapter.
- ~~4~~ 5. "Continuing Agreement" means an agreement that automatically renews unless terminated by one (1) party.

- ~~5.~~ 6. "Exigent Circumstances" means a law enforcement agency's good faith belief that an emergency involving danger of, or imminent threat of the destruction of evidence regarding, death or serious physical injury to any person requires the use of surveillance technology or the information it provides.
- ~~6.~~ 7. "Face Recognition Technology" means an automated or semi-automated process that: (A) assists in identifying or verifying an individual based on an individual's face; or (B) identifies or logs characteristics of an individual's face, head, or body to infer emotion, associations, expressions, or the location of an individual.
- ~~7.~~ 8. "Large-Scale Event" means an event attracting ten thousand (10,000) or more people with the potential to attract national media attention that provides a reasonable basis to anticipate that exigent circumstances may occur.
9. "Other Remote Biometric Recognition" means: (A) an automated or semi-automated process that (i) assists in identifying an individual, capturing information about an individual, or otherwise generating or assisting in generating information about an individual based on physiological, biological, or behavioral characteristics ascertained from a distance; (ii) uses voice recognition technology; or (iii) identifies or logs such characteristics to infer emotion, associations, activities, or the location of an individual; and (B) does not include identification based on fingerprints or palm prints that have been manually obtained during the course of a criminal investigation or detention.
- ~~8.~~ 10. "Personal Communication Device" means a mobile telephone, a personal digital assistant, a wireless capable tablet and a similar wireless two-way communications and/or portable internet accessing devices, whether procured or subsidized by a city entity or personally owned, that is used in the regular course of city business.
11. "Predictive Policing Technology" means computer algorithms that use preexisting data to forecast or predict places or times that have a high risk of crime, or individuals or groups who are likely to be connected to a crime. This definition does not include computer algorithms used solely to visualize, chart, or map past criminal activity (e.g. heat maps).
- ~~9.~~ 12. "Police Area" refers to each of the geographic districts assigned to a police commander and as such districts are amended from time to time.
- ~~10.~~ 13. "Surveillance" or "Surveil" means to observe or analyze the movements, behavior, data, or actions of individuals. Individuals include those whose identity can be revealed by license plate data when combined with any other record.
- ~~11.~~ 14. "Surveillance Technology" means any software, electronic device, system utilizing an electronic device, or similar technological tool used, designed, or primarily intended to

collect, retain, analyze, process, or share audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group. Examples of surveillance technology include, but is not limited to the following: cell site simulators (Stingrays); automatic license plate readers; gunshot detectors (ShotSpotter); facial recognition software; thermal imaging systems; body-worn cameras; social media analytics software; gait analysis software; video cameras that record audio or video, and transmit or can be remotely accessed. It also includes software designed to monitor social media services or forecast criminal activity or criminality, biometric identification hardware or software.

"Surveillance technology" does not include the following devices or hardware, unless they have been equipped with, or are modified to become or include, a surveillance technology as defined above:

- A. Routine office hardware, such as televisions, computers, credit card machines, badge readers, copy machines, and printers, that is in widespread use and will not be used for any surveillance or law enforcement functions;
- B. Parking Ticket Devices (PTDs);
- C. Manually-operated, non-wearable, handheld digital cameras, audio recorders, and video recorders that are not designed to be used surreptitiously and whose functionality is limited to manually capturing and manually downloading video and/or audio recordings;
- D. Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles;
- E. Manually-operated technological devices used primarily for internal municipal entity communications and are not designed to surreptitiously collect surveillance data, such as radios and email systems;
- F. City databases that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology, including payroll, accounting, or other fiscal databases.
- G. Medical equipment used to diagnose, treat, or prevent disease or injury.
- H. Police department interview room cameras.
- I. Police department case management and records management systems, including computer aided dispatch systems, and field-based reporting systems.
- J. Police department early warning systems.

- K. Personal communication devices that have not been modified beyond stock manufacturer capabilities in a manner described above, provided that any bundled Face Recognition Technology is only used for the sole purpose of user authentication in the regular course of conducting City business.
- L. Live Scan Machines (owned by Alameda County Sheriff but operated by Oakland Police personnel.)

~~12.~~ 15. "Surveillance Impact Report" means a publicly-released written report including at a minimum the following:

- A. Description: information describing the surveillance technology and how it works, including product descriptions and manuals from manufacturers;
- B. Purpose: information on the proposed purposes(s) for the surveillance technology;
- C. Location: the location(s) it may be deployed, using general descriptive terms, and crime statistics for any location(s);
- D. Impact: an assessment of the technology's adopted use policy and whether it is adequate in protecting civil rights and liberties and whether the surveillance technology was used or deployed, intentionally or inadvertently, in a manner that is discriminatory, viewpoint-based, or biased via algorithm;
- E. Mitigations: identify specific, affirmative technical and procedural measures that will be implemented to safeguard the public from each such impacts;
- F. Data Types and Sources: a list of all types and sources of data to be collected, analyzed, or processed by the surveillance technology, including "open source" data, scores, reports, logic or algorithm used, and any additional information derived therefrom;
- G. Data Security: information about the steps that will be taken to ensure that adequate security measures are used to safeguard the data collected or generated by the technology from unauthorized access or disclosure;
- H. Fiscal Cost: the fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, operative or proposed contract, and any current or potential sources of funding;
- I. Third Party Dependence: whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis;

- J. Alternatives: a summary of all alternative methods (whether involving the use of a new technology or not) considered before deciding to use the proposed surveillance technology, including the costs and benefits associated with each alternative and an explanation of the reasons why each alternative is inadequate; and,
 - K. Track Record: a summary of the experience (if any) other entities, especially government entities, have had with the proposed technology, including, if available, quantitative information about the effectiveness of the proposed technology in achieving its stated purpose in other jurisdictions, and any known adverse information about the technology (such as unanticipated costs, failures, or civil rights and civil liberties abuses).
- ~~13.~~ 16. "Surveillance Use Policy" means a publicly-released and legally enforceable policy for use of the surveillance technology that at a minimum specifies the following:
- A. Purpose: the specific purpose(s) that the surveillance technology is intended to advance;
 - B. Authorized Use: the specific uses that are authorized, and the rules and processes required prior to such use;
 - C. Data Collection: the information that can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including "open source" data;
 - D. Data Access: the category of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information;
 - E. Data Protection: the safeguards that protect information from unauthorized access, including encryption and access control mechanisms;
 - F. Data Retention: the time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period;
 - G. Public Access: how collected information can be accessed or used by members of the public, including criminal defendants;

- H. Third Party Data Sharing: if and how other city departments, bureaus, divisions, or non-city entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information;
 - I. Training: the training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology, and the category of staff that will provide the training;
 - J. Auditing and Oversight: the mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy; and
 - K. Maintenance: The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.
17. “Voice Recognition Technology” means the automated or semi-automated process that assists in identifying or verifying an individual based on the characteristics of an individual’s voice.

9.64.020 - Privacy Advisory Commission (PAC) notification and review requirements.

- 1. PAC Notification Required Prior to City Solicitation of Funds and Proposals for Surveillance Technology.
 - A. City staff shall notify the Chair of the Privacy Advisory Commission prior to:
 - 1. Seeking or soliciting funds for new surveillance technology or to replace existing surveillance technology that has not been previously approved by the City Council pursuant to the requirements of this Chapter, including but not limited to applying for a grant; or,
 - 2. Soliciting proposals with a non-city entity to acquire, share or otherwise use surveillance technology or the information it provides.
 - B. Upon notification by city staff, the Chair of the Privacy Advisory Commission shall place the item on the agenda at the next Privacy Advisory Commission meeting for discussion and possible action. At this meeting, city staff shall inform the Privacy Advisory Commission of the need for the funds or equipment, or shall

otherwise justify the action city staff will seek Council approval for pursuant to 9.64.030. The Privacy Advisory Commission may make a recommendation to the City Council by voting its approval to proceed, object to the proposal, recommend that the city staff modify the proposal, or take no action.

- C. Should the Privacy Advisory Commission not make a recommendation pursuant to 9.64.020 1.B., City staff may proceed and seek Council approval of the proposed surveillance technology initiative pursuant to the requirements of Section 9.64.030.
2. PAC Review Required for New Surveillance Technology Before City Council Approval.
 - A. Prior to seeking City Council approval under Section 9.64.030, city staff shall submit a surveillance impact report and a surveillance use policy for the proposed new surveillance technology initiative to the Privacy Advisory Commission for its review at a regularly noticed meeting. The surveillance impact report and surveillance use policy must address the specific subject matter specified for such reports as defined under 9.64.010.
 - B. The Privacy Advisory Commission shall recommend that the City Council adopt, modify, or reject the proposed surveillance use policy. If the Privacy Advisory Commission proposes that the Surveillance Use Policy be modified, the Privacy Advisory Commission shall propose such modifications to city staff. City staff shall present such modifications to City Council when seeking City Council approval under Section 9.64.030.
 - C. Failure by the Privacy Advisory Commission to make its recommendation on the item within ninety (90) days of submission shall enable the city entity to proceed to the City Council for approval of the item.
 3. PAC Review Requirements for Existing Surveillance Technology Before City Council Approval.
 - A. Prior to seeking City Council approval for existing city surveillance technology under Section 9.64.030 city staff shall submit a surveillance impact report and surveillance use policy to the Privacy Advisory Commission for its review at a regularly noticed meeting. The surveillance impact report and surveillance use policy must address the specific subject matter specified for such reports as defined under 9.64.010.

- B. Prior to submitting the surveillance impact report and proposed surveillance use policy as described above, city staff shall present to the Privacy Advisory Commission a list of surveillance technology possessed and/or used by the city.
- C. The Privacy Advisory Commission shall rank the items in order of potential impact to civil liberties.
- D. Within sixty (60) days of the Privacy Advisory Commission's action in 9.64.020.3 4.C., city staff shall submit at least one (1) surveillance impact report and proposed surveillance use policy per month the Privacy Advisory Commission for review, beginning with the highest-ranking items as determined by the Privacy Advisory Commission, and continuing thereafter each month until a policy has been submitted for each item on the list.

City staff, acting on behalf of a particular department, agency, bureau, or other subordinate division of the City, is not required to submit a new surveillance impact report and surveillance use policy, until the Privacy Advisory Commission has completed its recommendation and analysis on any outstanding surveillance technology that has been previously submitted from such department, agency, bureau, or other subordinate division of the City.
- E. Failure by the Privacy Advisory Commission to make its recommendation on any item within ninety (90) days of submission shall enable city staff to proceed to the City Council for approval of the item pursuant to Section 9.64.030.

9.64.030. - City Council approval requirements for new and existing surveillance technology.

- 1. City staff must obtain City Council approval prior to any of the following:
 - A. Accepting state or federal funds or in-kind or other donations for surveillance technology, except for surveillance technology that has already been approved by City Council and for which a corresponding use policy is in effect;
 - B. Acquiring new surveillance technology, or replacing existing surveillance technology that has not been previously approved by the City Council pursuant to the requirements of this Chapter, including but not limited to procuring such technology without the exchange of monies or consideration;
 - C. Using new surveillance technology, or using existing surveillance technology or the information it provides for a purpose, in a manner, or in a location not previously approved by the City Council pursuant to the requirements of this

Chapter. However, for surveillance technology that was acquired or was in use prior to enactment of this ordinance, such use may continue until the City Council votes to approve or reject the surveillance technology's corresponding surveillance use policy; or

- D. Entering into a continuing agreement or written agreement with a non-City entity to acquire, share or otherwise use surveillance technology or the information it provides, including data sharing agreements.
- E. Notwithstanding any other provision of this Section, nothing herein shall be construed to prevent, restrict or interfere with any person providing evidence or information derived from surveillance technology to a law enforcement agency for the purposes of conducting a criminal investigation or the law enforcement agency from receiving such evidence or information.

2. City Council Approval Process.

A. After the PAC notification and review requirements in Section 9.64.020 have been met, city staff seeking City Council approval shall schedule for City Council consideration and approval of the proposed surveillance impact report and proposed surveillance use policy, and include Privacy Advisory Commission recommendations ~~at least fifteen (15) days prior to a mandatory, properly noticed, germane public hearing.~~ City Council consideration and approval may only occur at a public meeting that has been noticed in conformance with the Oakland Sunshine Ordinance. hearing. City staff shall not unreasonably delay scheduling any item for City Council consideration and approval at the next earliest opportunity.

- B. The City Council shall only approve any action as provided in this Article after first considering the recommendation of the Privacy Advisory Commission, and subsequently making a determination that the benefits to the community of the surveillance technology outweigh the costs; that the proposal will safeguard civil liberties and civil rights; and that, in the City Council's judgment, no alternative with a lesser economic cost or impact on civil rights or civil liberties would be as effective.
- C. For approval of existing surveillance technology for which the Privacy Advisory Commission failed to make its recommendation within ninety (90) days of review as provided for under 9.64.020 3.E, if the City Council has not reviewed and approved such item within four (4) City Council meetings from when the item was initially scheduled for City Council consideration, the city shall cease its use of the surveillance technology until such review and approval occurs.

3. Surveillance Impact Reports and Surveillance Use Policies are Public Records. City staff shall make the Surveillance Impact Report and Surveillance Use Policy, as updated from time to time, available to the public as long as the city uses the surveillance technology in accordance with its request pursuant to Section 9.64.020 A.1.

9.64.035 - Use of unapproved technology during exigent circumstances or large-scale event.

1. City staff may temporarily acquire or use surveillance technology and the data derived from that use in a manner not expressly allowed by a surveillance use policy in two (2) types of circumstances without following the provisions of Section 9.64.030: (A) exigent circumstances, and (B) a large-scale event.
2. If city staff acquires or uses a surveillance technology in the two (2) circumstances pursuant to subdivision 1., the city staff shall:
 - A. Use the surveillance technology to solely respond to the exigent circumstances or large-scale event.
 - B. Cease using the surveillance technology when the exigent circumstances or large scale event ends.
 - C. Only keep and maintain data related to the exigent circumstances and dispose of any data that is not relevant to an ongoing investigation.
 - D. Following the end of the exigent circumstances or large-scale event, report that acquisition or use to the PAC at their next respective meetings for discussion and/or possible recommendation to the City Council in accordance with the Sunshine Ordinance, the Brown Act, and City Administrator deadlines.
3. Any technology temporarily acquired in exigent circumstances or during a large-scale event shall be returned within seven (7) days following its acquisition, or when the exigent circumstances end, whichever is sooner, unless the technology is submitted to the City Council for approval pursuant to Section 9.64.030 and is approved. If the agency is unable to comply with the seven-day timeline, the agency shall notify the City Council, who may grant an extension.

9.64.040 - Oversight following City Council approval.

1. By April 30th March 15th of each year, ~~or at the next closest regularly scheduled Privacy Advisory Commission meeting,~~ or no later than one year after adoption of a

Surveillance Use Policy, city staff must present a written annual surveillance report for Privacy Advisory Commission review for each approved surveillance technology item. If city staff is unable to meet the deadline, city staff shall notify the Privacy Advisory Commission in writing of staff's request to extend this period, and the reasons for that request. The Privacy Advisory Commission may grant a single extension of up to sixty (60) days to comply with this provision.

- A. After review by the Privacy Advisory Commission, city staff shall submit the annual surveillance report to the City Council.
 - B. The Privacy Advisory Commission shall recommend to the City Council that the benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded; that use of the surveillance technology cease; or propose modifications to the corresponding surveillance use policy that will resolve the concerns.
 - C. Failure by the Privacy Advisory Commission to make its recommendation on the item within ninety (90) days of submission shall enable the city entity to proceed to the City Council for approval of the annual surveillance report.
2. Based upon information provided in city staff's Annual Surveillance Report and after considering the recommendation of the Privacy Advisory Commission, the City Council shall re-visit its "cost benefit" analysis as provided in Section 9.64.030 2.B. and either uphold or set aside the previous determination. Should the City Council set aside its previous determination, the city's use of the surveillance technology must cease. Alternatively, City Council may require modifications to the Surveillance Use Policy that will resolve any deficiencies.

9.64.045 - Prohibition on City's acquisition and/or use of ~~face recognition technology~~ Biometric Surveillance Technology and Predictive Policing Technology.

- A. Notwithstanding any other provision of this Chapter (9.64), it shall be unlawful for the City or any City staff to obtain, retain, request, access, or use:
 1. Biometric Surveillance Technology; or
 2. Predictive Policing Technology; or
 3. Information obtained from either Biometric Surveillance Technology or Predictive Policing Technology.
- ~~1. Face recognition technology; or~~

- ~~2. Information obtained from face recognition technology.~~
- B. Only surveillance technology that uses biometric information in a manner that meets the definition of Biometric Surveillance Technology, as provided in Section 9.64.010, shall be prohibited.
- C. City staff's inadvertent or unintentional receipt, access of, or use of any information obtained from ~~face recognition technology~~ Biometric Surveillance Technology or Predictive Policing Technology shall not be a violation of this Section 9.64.045 provided that:
1. City staff did not request or solicit the receipt, access of, or use of such information; and
 2. City staff shall immediately destroy all copies of the information upon its discovery and shall not use the information for any purpose, unless retention or use of exculpatory evidence is required by law; and
 - ~~2.~~ 3. Upon discovery of such use, City staff logs such receipt, access, or use in its annual surveillance report as referenced by Section 9.64.040 a written report and submits such report at the next regularly scheduled meeting of the Privacy Advisory Commission for discussion and possible recommendation to the City Council. Such a report shall not include any personally identifiable information or other information the release of which is prohibited by law. In its report, City staff shall identify specific measures taken by the City to prevent the further transmission or use of any information inadvertently or unintentionally obtained through the use of such technologies; and
 4. After review by the Privacy Advisory Commission, city staff shall submit the report to the City Council.

9.64.050 - Enforcement.

1. Violations of this Article are subject to the following remedies:
 - A. Any violation of this Article, or of a surveillance use policy promulgated under this Article, constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in the Superior Court of the State of California to enforce this Article. An action instituted under this paragraph shall be brought against the respective city department, and the City of Oakland, and, if necessary to

effectuate compliance with this Article or a surveillance use policy (including to expunge information unlawfully collected, retained, or shared thereunder), any other governmental agency with possession, custody, or control of data subject to this Article, to the extent permitted by law.

- B. Any person who has been subjected to a surveillance technology in violation of this Article, or about whom information has been obtained, retained, accessed, shared, or used in violation of this Article or of a surveillance use policy promulgated under this Article, may institute proceedings in the Superior Court of the State of California against the City of Oakland and shall be entitled to recover actual damages (but not less than liquidated damages of one thousand dollars (\$1,000.00) or one hundred dollars (\$100.00) per day for each day of violation, whichever is greater).
- C. A court shall award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in an action brought under paragraphs A. or B.
- D. Violations of this Article by a city employee shall result in consequences that may include retraining, suspension, or termination, subject to due process requirements and in accordance with any memorandums of understanding with employee bargaining units.

9.64.060 - Secrecy of surveillance technology.

It shall be unlawful for the city to enter into any surveillance-related contract or other agreement that conflicts with the provisions of this Article, and any conflicting provisions in such future contracts or agreements, including but not limited to non-disclosure agreements, shall be deemed void and legally unenforceable.

To the extent permitted by law, the city shall publicly disclose all of its surveillance-related contracts, including any and all related non-disclosure agreements, if any, regardless of any contract terms to the contrary.

9.64.070 - Whistleblower protections.

- 1. Neither the city nor anyone acting on behalf of the city may take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee or

applicant for employment, including but not limited to discriminating with respect to compensation, terms and conditions of employment, access to information, restrictions on due process rights, or civil or criminal liability, because:

- A. The employee or applicant was perceived to, about to, or assisted in any lawful disclosure of information concerning the funding, acquisition, or use of a surveillance technology or surveillance data based upon a good faith belief that the disclosure evidenced a violation of this Article; or
 - B. The employee or applicant was perceived to, about to, or assisted or participated in any proceeding or action to carry out the purposes of this Article.
2. It shall be grounds for disciplinary action for a city employee or anyone else acting on behalf of the city to retaliate against another city employee or applicant who makes a good-faith complaint that there has been a failure to comply with any surveillance use policy or administrative instruction promulgated under this Article.
 3. Any employee or applicant who is injured by a violation of this Section may institute a proceeding for monetary damages and injunctive relief against the city in any court of competent jurisdiction.

SECTION 3. Severability. If any section, subsection, sentence, clause or phrase of this Ordinance is for any reason held to be invalid or unconstitutional by decision of any court of competent jurisdiction, such decision shall not affect the validity of the remaining portions of the Chapter. The City Council hereby declares that it would have passed this Ordinance and each section, subsection, clause or phrase thereof irrespective of the fact that one or more other sections, subsections, clauses or phrases may be declared invalid or unconstitutional

SECTION 4. California Environmental Quality Act. The City Council hereby finds and determines that this action is exempt from environmental review under the California Environmental Quality Act (CEQA) pursuant to: (1) CEQA Guidelines Section 15061(b)(3), Review for Exemptions – General Rule, in that it can be seen with certainty that there is no possibility for this action to have a significant effect on the environment; and (2) CEQA Guidelines Section 15378(b)(5), since this action does not constitute a “project” within the meaning of CEQA and instead relates to “[o]rganizational or administrative activities of [the City] that will not result in direct or indirect physical changes in the environment.”

SECTION 5. Effective Date. This ordinance shall become effective immediately on final adoption if it receives six or more affirmative votes; otherwise it shall become effective upon the seventh day after final adoption.

IN COUNCIL, OAKLAND, CALIFORNIA,

PASSED BY THE FOLLOWING VOTE:

AYES -FORTUNATO BAS, GALLO, GIBSON MCELHANEY, KALB, REID, TAYLOR,
THAO AND PRESIDENT KAPLAN

NOES –

ABSENT –

ABSTENTION –

ATTEST: _____

ASHA REED
Acting City Clerk and Clerk of the
Council of the City of Oakland, California

Date of Attestation: _____

3006267



CITY OF CARMEL-BY-THE-SEA COMMUNITY MEETING Staff Report

October 24, 2024

TO:	Community Meeting Members
SUBMITTED BY:	Chip Rerig, City Administrator
SUBJECT:	Presentation and other documents received after agenda posting

RECOMMENDATION:

BACKGROUND/SUMMARY:

FISCAL IMPACT:

PRIOR CITY COUNCIL ACTION:

ATTACHMENTS:

- Carmel PD Crime Reporting_10-23-24
- About Flock ALPR
- Flock Group Services Agreement
- Flock Camera Questions from previous Ad Hoc meetings

CLASSIFICATION	PROPERTY STOLEN BY CLASSIFICATION		Attachment 1 VALUE OF PROPERTY STOLEN
	DA EN	NUMBER ACTUAL OFFENSES	
1. Murder & Non-neg Manslaughter	12		
2. Rape (Total)	20	3	
3. Robbery			
A. Highway	31	1	
B. Commercial House	32	1	53400
C. Gas/Service Station	33		
D. Convenience Store	34		
E. Residence	35	1	
F. Bank	36		
G. Miscellaneous	37	2	20
TOTAL ROBBERY	30	5	53420
5. Burglary - Breaking/Entering			
(A) Residence (Dwelling)			
1. Night (6PM - 6 AM)	51	5	1353
2. Day (6AM - 6 PM)	52	1	
3. Unknown	53	6	24964
(B) Non-Residence (Store, etc)			
1. Night (6PM - 6 AM)	54	4	
2. Day (6AM - 6 PM)	55	1	4050
3. Unknown	56	3	239
TOTAL BURGLARY	50	20	30606
6. Larceny - Theft			
A. Over \$400	64	36	107685
B. \$200 through \$400	61	11	3000
C. \$50 to \$200	62	9	1134
D. Under \$50	63	17	731
TOTAL LARCENY	60	73	112550
7. Motor Vehicle Theft	70	2	10200
Grand Total - ALL ITEMS	77	100	206776
Additional Analysis of 6 & 7			
6X. Nature of Items Under 6			
A. Pocket-Picking	81		
B. Purse-Snatching	82	1	360
C. Shoplifting	83	4	3022
D. From Motor Vehicle	84	27	21410
E. Motor Vehicle Parts	85	2	1250
F. Bicycles	86	11	12265
G. From Buildings	87	11	57985
H. From Coin Machines	88		
I. All Other	89	17	16258
TOTAL LARCENIES (Items 6)	80	73	112550
7X. Motor Vehicles Recovered			
A. Stolen Local Recovery Local	91	1	
B. Stolen Local Recovery Other	92		
C. Total Local Vehs. Recovered	90	1	
D. Stolen Other Recovery Local	93	1	

CARMEL-BY-THE-SEA POLICE DEPARTMENT

CHIEF PAUL TOMASI

Prepared By : ALMARIO, DAWN
Reporting Month & Year : 20

NCIC Identifier : 2701
Date Prepared : 10/23/2024

Preparer Title : PSO
Population Served : 0004081

RETURN A - MONTHLY RETURN OF OFFENSES KNOWN TO POLICE

Attachment 1

CLASSIFICATION OF OFFENSES	DA EN	OFFENSES REPORTED	UNFOUNDED	ACTUAL OFFENSES	ARREST CLEARANCE	UNDER 18 CLEARANCE
1. CRIMINAL HOMICIDE						
A. MURDER AND NONNEG	11					
B. MANSLAUGHTER NEG	12					
2. RAPE (Total)	20	3		3	3	
A. Rape	21	3		3	3	
B. Attempts	22					
Historical Rape						
3. ROBBERY TOTAL	30	5		5	4	
A. Firearm	31					
B. Knife	32					
C. Other Weapon	33	2		2	1	
D. Strong-Arm	34	3		3	3	
4. ASSAULT TOTAL	40	18		18	8	1
A. Firearm	41	1		1	1	
B. Knife	42	1		1		
C. Other Weapon	43	1		1		
D. Hands Aggravated	44	5		5	3	
E. Other Not Aggravated	45	10		10	4	1
5. BURGLARY TOTAL	50	20		20	4	
A. Forcible Entry	51	10		10	3	
B. Unlawful Entry	52	4		4	1	
C. Attempted Forcible	53	6		6		
6. LARCENY TOTAL	60	73		73	10	1
7. MOTOR VEH THEFT TOTAL	70	2		2	1	
A. Autos	71	1		1	1	
B. Trucks & Buses	72					
C. Other Vehicles	73	1		1		
GRAND TOTAL	77	121		121	30	2

() NO SUPPLEMENTARY HOMICIDE
 () NO SUPPLEMENT FOR PROPERTY
 () NO OFFICERS KILLED/ASSAULTED

() NO ARRESTS UNDER 18 YEARS
 () NO ARRESTS 18 YEARS OR OVER
 () NO ARSON OFFENSES

CARMEL-BY-THE-SEA POLICE DEPARTMENT

CHIEF PAUL TOMASI

Reporting Month & Year : 20

NCIC Identifier : 2701

Population Served : 0004081

Prepared By : ALMARIO, DAWN

Date Prepared : 10/23/2024

Preparer Title : PSO

CLASSIFICATION	DA EN	PROPERTY STOLEN BY CLASSIFICATION NUMBER ACTUAL OFFENSES	Attachment 1 VALUE OF PROPERTY STOLEN
1. Murder & Non-neg Manslaughter	12		
2. Rape (Total)	20		
3. Robbery			
A. Highway	31		
B. Commercial House	32	1	1347950
C. Gas/Service Station	33		
D. Convenience Store	34		
E. Residence	35		
F. Bank	36		
G. Miscellaneous	37	1	1700
TOTAL ROBBERY	30	2	1349650
5. Burglary - Breaking/Entering			
(A) Residence (Dwelling)			
1. Night (6PM - 6 AM)	51	3	3700
2. Day (6AM - 6 PM)	52	3	161
3. Unknown	53	4	7250
(B) Non-Residence (Store, etc)			
1. Night (6PM - 6 AM)	54	3	112257
2. Day (6AM - 6 PM)	55	1	188
3. Unknown	56	1	
TOTAL BURGLARY	50	15	123556
6. Larceny - Theft			
A. Over \$400	64	34	64029
B. \$200 through \$400	61	13	3220
C. \$50 to \$200	62	13	1286
D. Under \$50	63	5	130
TOTAL LARCENY	60	65	68665
7. Motor Vehicle Theft	70		1
Grand Total - ALL ITEMS	77	82	1541872
Additional Analysis of 6 & 7			
6X. Nature of Items Under 6			
A. Pocket-Picking	81	1	154
B. Purse-Snatching	82	1	199
C. Shoplifting	83	12	7721
D. From Motor Vehicle	84	15	16178
E. Motor Vehicle Parts	85	4	2461
F. Bicycles	86	4	15700
G. From Buildings	87	6	13128
H. From Coin Machines	88		
I. All Other	89	22	13124
TOTAL LARCENIES (Items 6)	80	65	68665
7X. Motor Vehicles Recovered			
A. Stolen Local Recovery Local	91		
B. Stolen Local Recovery Other	92		
C. Total Local Vehs. Recovered	90		
D. Stolen Other Recovery Local	93		

CARMEL-BY-THE-SEA POLICE DEPARTMENT

CHIEF PAUL TOMASI

Prepared By: ALMARIO, DAWN
Reporting Month & Year: 21

NCIC Identifier: 2701
Date Prepared: 10/23/2024

Preparer Title: PSO
Population Served: 0004081

RETURN A - MONTHLY RETURN OF OFFENSES KNOWN TO POLICE

Attachment 1

CLASSIFICATION OF OFFENSES	DA EN	OFFENSES REPORTED	UNFOUNDED	ACTUAL OFFENSES	ARREST CLEARANCE	UNDER 18 CLEARANCE
1. CRIMINAL HOMICIDE						
A. MURDER AND NONNEG	11					
B. MANSLAUGHTER NEG	12					
2. RAPE (Total)	20					
A. Rape	21					
B. Attempts	22					
Historical Rape						
3. ROBBERY TOTAL	30	2		2	1	
A. Firearm	31					
B. Knife	32					
C. Other Weapon	33					
D. Strong-Arm	34	2		2	1	
4. ASSAULT TOTAL	40	22		22	12	
A. Firearm	41	1		1		
B. Knife	42					
C. Other Weapon	43					
D. Hands Aggravated	44	10		10	6	
E. Other Not Aggravated	45	11		11	6	
5. BURGLARY TOTAL	50	15		15	6	
A. Forcible Entry	51	5		5	2	
B. Unlawful Entry	52	7		7	3	
C. Attempted Forcible	53	3		3	1	
6. LARCENY TOTAL	60	65		65	8	
7. MOTOR VEH THEFT TOTAL	70					
A. Autos	71					
B. Trucks & Buses	72					
C. Other Vehicles	73					
GRAND TOTAL	77	104		104	27	

() NO SUPPLEMENTARY HOMICIDE
 () NO SUPPLEMENT FOR PROPERTY
 () NO OFFICERS KILLED/ASSAULTED

() NO ARRESTS UNDER 18 YEARS
 () NO ARRESTS 18 YEARS OR OVER
 () NO ARSON OFFENSES

CARMEL-BY-THE-SEA POLICE DEPARTMENT

CHIEF PAUL TOMASI

Reporting Month & Year : 21

NCIC Identifier : 2701

Population Served : 0004081

Prepared By : ALMARIO, DAWN

Date Prepared : 10/23/2024

Preparer Title : PSO

CLASSIFICATION	DA EN	PROPERTY STOLEN BY CLASSIFICATION NUMBER ACTUAL OFFENSES	Attachment 1 VALUE OF PROPERTY STOLEN
1. Murder & Non-neg Manslaughter	12		
2. Rape (Total)	20	1	
3. Robbery			
A. Highway	31	2	542
B. Commercial House	32		
C. Gas/Service Station	33		
D. Convenience Store	34		
E. Residence	35		
F. Bank	36		
G. Miscellaneous	37		
TOTAL ROBBERY	30	2	542
5. Burglary - Breaking/Entering			
(A) Residence (Dwelling)			
1. Night (6PM - 6 AM)	51		
2. Day (6AM - 6 PM)	52	1	
3. Unknown	53	2	9201
(B) Non-Residence (Store, etc)			
1. Night (6PM - 6 AM)	54	5	16217
2. Day (6AM - 6 PM)	55	3	16275
3. Unknown	56	1	
TOTAL BURGLARY	50	12	41693
6. Larceny - Theft			
A. Over \$400	64	41	553088
B. \$200 through \$400	61	2	541
C. \$50 to \$200	62	8	947
D. Under \$50	63	10	148
TOTAL LARCENY	60	61	554724
7. Motor Vehicle Theft	70		
Grand Total - ALL ITEMS	77	75	596959
Additional Analysis of 6 & 7			
6X. Nature of Items Under 6			
A. Pocket-Picking	81	1	839
B. Purse-Snacthing	82	3	1045
C. Shoplifting	83	15	28611
D. From Motor Vehicle	84	12	14558
E. Motor Vehicle Parts	85	2	1025
F. Bicycles	86	1	700
G. From Buildings	87	10	460590
H. From Coin Machines	88		
I. All Other	89	17	47356
TOTAL LARCENIES (Items 6)	80	61	554724
7X. Motor Vehicles Recovered			
A. Stolen Local Recovery Local	91		
B. Stolen Local Recovery Other	92		
C. Total Local Vehs. Recovered	90		
D. Stolen Other Recovery Local	93		

CARMEL-BY-THE-SEA POLICE DEPARTMENT

CHIEF PAUL TOMASI

Prepared By : ALMARIO, DAWN
Reporting Month & Year : 22

NCIC Identifier : 2701
Date Prepared : 10/23/2024

Preparer Title : PSO
Population Served : 0004081

RETURN A - MONTHLY RETURN OF OFFENSES KNOWN TO POLICE

Attachment 1

CLASSIFICATION OF OFFENSES	DA EN	OFFENSES REPORTED	UNFOUNDED	ACTUAL OFFENSES	ARREST CLEARANCE	UNDER 18 CLEARANCE
1. CRIMINAL HOMICIDE						
A. MURDER AND NONNEG	11					
B. MANSLAUGHTER NEG	12					
2. RAPE (Total)	20	1		1		
A. Rape	21	1		1		
B. Attempts	22					
Historical Rape						
3. ROBBERY TOTAL	30	2		2		
A. Firearm	31					
B. Knife	32					
C. Other Weapon	33					
D. Strong-Arm	34	2		2		
4. ASSAULT TOTAL	40	20		20	5	2
A. Firearm	41	1		1		
B. Knife	42					
C. Other Weapon	43	1		1		
D. Hands Aggravated	44	5		5	3	1
E. Other Not Aggravated	45	13		13	2	1
5. BURGLARY TOTAL	50	12		12	4	
A. Forcible Entry	51	4		4	2	
B. Unlawful Entry	52	6		6	2	
C. Attempted Forcible	53	2		2		
6. LARCENY TOTAL	60	61		61	7	
7. MOTOR VEH THEFT TOTAL	70					
A. Autos	71					
B. Trucks & Buses	72					
C. Other Vehicles	73					
GRAND TOTAL	77	96		96	16	2

() NO SUPPLEMENTARY HOMICIDE
 () NO SUPPLEMENT FOR PROPERTY
 () NO OFFICERS KILLED/ASSAULTED

() NO ARRESTS UNDER 18 YEARS
 () NO ARRESTS 18 YEARS OR OVER
 () NO ARSON OFFENSES

CARMEL-BY-THE-SEA POLICE DEPARTMENT

CHIEF PAUL TOMASI

Reporting Month & Year : 22

NCIC Identifier : 2701

Population Served : 0004081

Prepared By : ALMARIO, DAWN

Date Prepared : 10/23/2024

Preparer Title : PSO

CLASSIFICATION	PROPERTY STOLEN BY CLASSIFICATION		Attachment 1
	DA EN	NUMBER ACTUAL OFFENSES	VALUE OF PROPERTY STOLEN
1. Murder & Non-neg Manslaughter	12		
2. Rape (Total)	20	2	
3. Robbery			
A. Highway	31		
B. Commercial House	32		
C. Gas/Service Station	33		
D. Convenience Store	34		
E. Residence	35		
F. Bank	36		
G. Miscellaneous	37		
TOTAL ROBBERY	30		
5. Burglary - Breaking/Entering			
(A) Residence (Dwelling)			
1. Night (6PM - 6 AM)	51	1	
2. Day (6AM - 6 PM)	52	2	5002
3. Unknown	53	4	2195
(B) Non-Residence (Store, etc)			
1. Night (6PM - 6 AM)	54	4	164098
2. Day (6AM - 6 PM)	55	3	35700
3. Unknown	56	1	3600
TOTAL BURGLARY	50	15	210595
6. Larceny - Theft			
A. Over \$400	64	17	137621
B. \$200 through \$400	61	5	1815
C. \$50 to \$200	62	6	700
D. Under \$50	63	7	83
TOTAL LARCENY	60	35	140219
7. Motor Vehicle Theft	70	1	4000
Grand Total - ALL ITEMS	77	51	354814
Additional Analysis of 6 & 7			
6X. Nature of Items Under 6			
A. Pocket-Picking	81		
B. Purse-Snatching	82		
C. Shoplifting	83	6	1640
D. From Motor Vehicle	84	10	5027
E. Motor Vehicle Parts	85	4	5951
F. Bicycles	86	1	7249
G. From Buildings	87	7	19642
H. From Coin Machines	88		
I. All Other	89	7	100710
TOTAL LARCENIES (Items 6)	80	35	140219
7X. Motor Vehicles Recovered			
A. Stolen Local Recovery Local	91		
B. Stolen Local Recovery Other	92		
C. Total Local Vehs. Recovered	90		
D. Stolen Other Recovery Local	93		

CARMEL-BY-THE-SEA POLICE DEPARTMENT

CHIEF PAUL TOMASI

Prepared By : ALMARIO, DAWN
Reporting Month & Year : 23

NCIC Identifier : 2701
Date Prepared : 10/23/2024

Preparer Title : PSO
Population Served : 0004081

RETURN A - MONTHLY RETURN OF OFFENSES KNOWN TO POLICE

CLASSIFICATION OF OFFENSES	DA EN	OFFENSES REPORTED	UNFOUNDED	ACTUAL OFFENSES	ARREST CLEARANCE	UNDER 18 CLEARANCE
1. CRIMINAL HOMICIDE						
A. MURDER AND NONNEG	11					
B. MANSLAUGHTER NEG	12					
2. RAPE (Total)	20	2		2		
A. Rape	21	2		2		
B. Attempts	22					
Historical Rape						
3. ROBBERY TOTAL	30					
A. Firearm	31					
B. Knife	32					
C. Other Weapon	33					
D. Strong-Arm	34					
4. ASSAULT TOTAL	40	13		13	1	
A. Firearm	41					
B. Knife	42					
C. Other Weapon	43					
D. Hands Aggravated	44	4		4		
E. Other Not Aggravated	45	9		9	1	
5. BURGLARY TOTAL	50	15		15	1	
A. Forcible Entry	51	3		3		
B. Unlawful Entry	52	11		11	1	
C. Attempted Forcible	53	1		1		
6. LARCENY TOTAL	60	35		35		
7. MOTOR VEH THEFT TOTAL	70	1		1		
A. Autos	71					
B. Trucks & Buses	72	1		1		
C. Other Vehicles	73					
GRAND TOTAL	77	66		66	2	

() NO SUPPLEMENTARY HOMICIDE
 () NO SUPPLEMENT FOR PROPERTY
 () NO OFFICERS KILLED/ASSAULTED

() NO ARRESTS UNDER 18 YEARS
 () NO ARRESTS 18 YEARS OR OVER
 () NO ARSON OFFENSES

CARMEL-BY-THE-SEA POLICE DEPARTMENT

CHIEF PAUL TOMASI

Reporting Month & Year : 23

NCIC Identifier : 2701

Population Served : 0004081

Prepared By : ALMARIO, DAWN

Date Prepared : 10/23/2024

Preparer Title : PSO

CLASSIFICATION	PROPERTY STOLEN BY CLASSIFICATION		Attachment 1
	DA EN	NUMBER ACTUAL OFFENSES	VALUE OF PROPERTY STOLEN
1. Murder & Non-neg Manslaughter	12		
2. Rape (Total)	20		
3. Robbery			
A. Highway	31		
B. Commercial House	32		
C. Gas/Service Station	33		
D. Convenience Store	34		
E. Residence	35		
F. Bank	36		
G. Miscellaneous	37		
TOTAL ROBBERY	30		
5. Burglary - Breaking/Entering			
(A) Residence (Dwelling)			
1. Night (6PM - 6 AM)	51	1	
2. Day (6AM - 6 PM)	52		
3. Unknown	53	2	201
(B) Non-Residence (Store, etc)			
1. Night (6PM - 6 AM)	54	3	1665
2. Day (6AM - 6 PM)	55		
3. Unknown	56	1	6811
TOTAL BURGLARY	50	7	8677
6. Larceny - Theft			
A. Over \$400	64	29	70988
B. \$200 through \$400	61	4	899
C. \$50 to \$200	62	2	275
D. Under \$50	63	8	85
TOTAL LARCENY	60	43	72247
7. Motor Vehicle Theft	70		1
Grand Total - ALL ITEMS	77	50	80925
Additional Analysis of 6 & 7			
6X. Nature of Items Under 6			
A. Pocket-Picking	81	3	4075
B. Purse-Snatching	82		
C. Shoplifting	83	6	14381
D. From Motor Vehicle	84	20	41511
E. Motor Vehicle Parts	85	3	945
F. Bicycles	86		
G. From Buildings	87	4	3580
H. From Coin Machines	88	1	350
I. All Other	89	6	7405
TOTAL LARCENIES (Items 6)	80	43	72247
7X. Motor Vehicles Recovered			
A. Stolen Local Recovery Local	91		
B. Stolen Local Recovery Other	92		
C. Total Local Vehs. Recovered	90		
D. Stolen Other Recovery Local	93		

CARMEL-BY-THE-SEA POLICE DEPARTMENT

CHIEF PAUL TOMASI

Prepared By : ALMARIO, DAWN
 Reporting Month & Year : 24

NCIC Identifier : 2701
 Date Prepared : 10/23/2024

Preparer Title : PSO
 Population Served : 0004081

RETURN A - MONTHLY RETURN OF OFFENSES KNOWN TO POLICE

CLASSIFICATION OF OFFENSES	DA EN	OFFENSES REPORTED	UNFOUNDED	ACTUAL OFFENSES	ARREST CLEARANCE	UNDER 18 CLEARANCE
1. CRIMINAL HOMICIDE						
A. MURDER AND NONNEG	11					
B. MANSLAUGHTER NEG	12					
2. RAPE (Total)	20					
A. Rape	21					
B. Attempts	22					
Historical Rape						
3. ROBBERY TOTAL	30					
A. Firearm	31					
B. Knife	32					
C. Other Weapon	33					
D. Strong-Arm	34					
4. ASSAULT TOTAL	40	11		11	2	
A. Firearm	41					
B. Knife	42	1		1		
C. Other Weapon	43	1		1		
D. Hands Aggravated	44	2		2	1	
E. Other Not Aggravated	45	7		7	1	
5. BURGLARY TOTAL	50	7		7		
A. Forcible Entry	51	2		2		
B. Unlawful Entry	52	4		4		
C. Attempted Forcible	53	1		1		
6. LARCENY TOTAL	60	43		43	5	
7. MOTOR VEH THEFT TOTAL	70					
A. Autos	71					
B. Trucks & Buses	72					
C. Other Vehicles	73					
GRAND TOTAL	77	61		61	7	

() NO SUPPLEMENTARY HOMICIDE
 () NO SUPPLEMENT FOR PROPERTY
 () NO OFFICERS KILLED/ASSAULTED

() NO ARRESTS UNDER 18 YEARS
 () NO ARRESTS 18 YEARS OR OVER
 () NO ARSON OFFENSES

CARMEL-BY-THE-SEA POLICE DEPARTMENT

CHIEF PAUL TOMASI

Reporting Month & Year : 24

NCIC Identifier : 2701

Population Served : 0004081

Prepared By : ALMARIO, DAWN

Date Prepared : 10/23/2024

Preparer Title : PSO

About Automatic License Plate Readers (ALPR)

The Problem: Violent Crime Is Not Going Away

Nationwide, cities are experiencing a disturbing rise in homicides and violence. The FBI's 2020 Crime Report shows a 30% increase in homicides from 2019 to 2020, the largest single-year increase recorded.

Over two-thirds of the country's most populous cities saw even more homicides in 2021.

One Solution: Technology that Detects Objective Evidence to Clear More Cases

Automated License Plate Readers (ALPR) capture computer-readable images of license plates and vehicles, allowing officers to compare plate numbers against those of stolen cars or wanted individuals on a crime database like the NCIC.

ALPR devices assist law enforcement in solving crime in two ways:

- Proactive - ALPR devices provide real-time alerts when a vehicle that is stolen or associated with a known suspect is detected.
- Investigative - ALPR cameras help determine whether and which vehicle(s) were at the scene of a crime.

Is ALPR effective ?

According to the National Conference of State Legislatures, when employed ethically and objectively, ALPRs are an effective tool for law enforcement, cutting down on the time required for investigations and acting as a force multiplier. In 2011, a study by the Police Executive Research Forum concluded that ALPRs used by the Mesa, Ariz., Police Department resulted in "nearly 3 times as many 'hits' for stolen vehicles, and twice as many vehicle recoveries."

Communities with ALPR systems report crime reductions of up to 70 percent. In some areas, that included a 60 percent reduction in non-residential burglaries, 80 percent reduction in residential burglary, and a 40 percent reduction in robberies.

ALPR Provides Objective Evidence While Protecting Privacy

ALPR does not include facial recognition capabilities and does not capture personally identifiable information (PII). While eyewitnesses and individual officers are subject to inherent human bias, ALPR cameras capture wholly-objective images of vehicles and license plates, providing a clear and actionable investigative lead.

ALPR Use Cases Include:

- **AMBER Alerts:** License plate readers in metro Atlanta were able to find a vehicle containing a kidnapped one-year-old, who had been taken from his mother at random off the street. The child was recovered unharmed. Some ALPR systems integrate directly with the National Center for Missing and Exploited Children's AMBER Alert system, sending real-time alerts to officers in seconds. [[New information released about 1-year-old's kidnapping](#)]
- **Silver Alerts:** Knoxville Police were able to locate a missing elderly man who suffers from dementia after he drove away in a family vehicle. ALPR technology has helped solve hundreds of Silver Alerts across the country. [[Missing man with dementia found using Flock camera](#)]
- **Firearm violence:** The Las Vegas Trail, a high-crime area in Fort Worth, TX, saw violent crime decrease by 22% in 2021 compared with the first nine months of 2019. Fort Worth Police attributed this drop partially to the license plate reader system implemented in the neighborhood during the same period of time. [[Crime is down 22% in Fort Worth's Las Vegas Trail. How neighbors and police made it safer](#)]
- **Organized theft:** Grafton, a growing village with a bustling retail district, is dealing with increased organized retail theft – Two-thirds of all the crimes reported to Grafton police in 2020 were retail thefts. Grafton Police have implemented a license plate reader system to identify vehicles that have been involved in thefts or have been stolen themselves. In one week alone, they recovered three stolen vehicles with drivers planning to engage in retail theft. [[Losses mount as retailers fight theft rings, accuse online storefronts of doing little to stop resale of stolen goods](#)]

flock safety

Sole Source Letter for Flock Safety™ ALPR Cameras and Solution

Flock Safety is the sole manufacturer and developer of the Flock Safety ALPR Camera. Flock Safety is also the sole provider of the comprehensive monitoring, processing, and machine vision services which integrate with the Flock Safety ALPR Camera.

The Flock Safety ALPR camera and devices are the only Law Enforcement Grade ALPR System to offer the following combination of proprietary features:

1. Vehicle Fingerprint Technology™:
 - Patented proprietary machine vision to analyze vehicle license plate, state recognition, and vehicle attributes such as color, type, make and objects (roof rack, bumper stickers, etc.) based on image analytics (not car registration data)
 - Machine vision to capture and identify characteristics of vehicles with a paper license plate and vehicles with the absence of a license plate
 - Ability to 'Save Search' based on description of vehicles using our patented Vehicle Fingerprint Technology without the need for a license plate, and set up alerts based on vehicle description
 - Only LPR provider with "Visual Search" which can transform digital images from any source into an investigative lead by finding matching vehicles based on the vehicle attributes in the uploaded photo
 - Falcon Flex™: an infrastructure-free, location-flexible license plate reader camera that is easy to self install. Falcon Flex ties seamlessly into the Flock ecosystem with a small and lightweight camera with the ability to read up to 30,000 license plates and vehicle attributes on a single battery charge

 2. Integrated Cloud-Software & Hardware Platform:
 - Ability to capture two (2+) lanes of traffic simultaneously with a single camera from a vertical mass
 - Best in class ability to capture and process up to 30,000 vehicles per day with a single camera powered exclusively by solar power
 - Wireless deployment of solar powered license plate reading cameras with integrated cellular communication weighing less than 5lbs and able to be powered solely by a solar panel of 60W or less
 - Web based footage retrieval tool with filtering capabilities such as vehicle color, vehicle type, vehicle manufacturer, partial or full license plate, state of license plate, and object detection
 - Utilizes motion capture to start and stop recording without the need for a reflective plate
-

flock safety

- Motion detection allows for unique cases such as bicycle capture, ATV, motorcycle, etc.
 - On device machine processing to limit LTE bandwidth consumption
 - Cloud storage of footage
 - Covert industrial design for minimizing visual pollution
3. Transparency & Ethical Product Design:
- One-of-a-kind "Transparency Portal" public-facing dashboard that details the policies in place by the purchaser, as well as automatically updated metrics from the Flock system
 - Built-in integration with NCMEC to receive AMBER Alerts to find missing children
 - Privacy controls to enable certain vehicles to "opt-out" of being captured
4. Integrated Audio & Gunshot Detection:
- Natively integrated audio detection capabilities utilizing machine learning to recognize audio signatures typical of crimes in progress (e.g., gunshots)
5. Live Video Integration:
- Ability to apply computer vision to third-party cameras using Wing™ LPR, transforming them to evidence capture devices using the same Vehicle Fingerprint technology offered on the Flock Safety Falcon™ ALPR cameras
 - Wing™ Livestream integrates live stream traffic cameras, publicly or privately owned livestream security cameras into one cloud-based situational awareness dashboard to increase response time in mission-critical incidents
 - Manage various government intelligence including ALPR, livestream cameras, CAD, automatic vehicle location (AVL) on Flock Safety's Wing™ Suite
 - Access Wing™ Replay to unlock enhanced situational awareness with 7-day footage retention, Hot List Live Video Instant Replay, and downloadable MP4
6. Partnerships:
- Flock Safety is the only LPR provider to officially partner with AXON to be natively and directly integrated into Evidence.com
 - Flock Safety is the only LPR provider to be fully integrated into a dynamic network of Axon's Fleet 3 mobile ALPR cameras for patrol cars and Flock Safety's Falcon cameras
 - Access to additional cameras purchased by our HOA and private business partners, means an ever-increasing amount of cameras and data at no additional cost
-

flock safety

7. Warranty & Service:

- Lifetime maintenance and support included in subscription price
- Flock Safety is the only fully integrated ALPR one-stop solution from production of the camera to delivery and installation
- Performance monitoring software to predict potential failures, obstructions, tilts, and other critical or minor issues

Thank you,



Garrett Langley CEO, Flock Safety

flock safety

Attachment 2

Let's defeat crime together

Help your city reduce crime with cameras that see like a detective

"Flock Safety made my job easy. The system was up and running in just a few weeks, and has proven to help our police department find the evidence to solve more crime."

City Manager in Ohio

Flock Safety provides an affordable, infrastructure-free automatic license plate reading (ALPR) camera system for cities who want to reduce crime within a principled framework. Unlike traditional ALPR, Flock uses Vehicle Fingerprint™ technology to transform hours of footage into a searchable database to find the single piece of evidence needed, even when a license plate isn't visible.

Not your average security cameras

Infrastructure-Free and Discreet Design

With solar power and LTE connectivity, we can install the devices almost anywhere. And the beautiful design means it will blend in with your city's aesthetic.

Safety-as-a-Service

We install and maintain the devices, so you can focus on running the city. That means we will support you from procurement, through permitting, and even preparing you to present this project to the city council.

Vehicle Fingerprint Technology

Your officers can find vehicle evidence by vehicle type, make, color, license plate state, missing and covered plates, and other unique features like bumper stickers, decals, and roof racks.



Join 2500+ cities using Flock Safety to eliminate crime



Detect

objective evidence your police need to solve crime



Decode

footage with machine learning so your police can investigate



Deliver

real-time alerts to police if a wanted or stolen vehicle drives by

Public Safety Technology Built with Principles

You own the footage

We won't share it or sell it. It's 100% yours for your law enforcement to use to solve crime.

Protect resident privacy

All data automatically deletes by default every 30 days on a rolling basis and is encrypted with AES-256 encryption.

Promote transparency and accountability

Flock provides a transparency portal to share data with your community about how the devices work on an ongoing basis. Flock requires an investigative reason to search and proactively provides an audit report to city leadership.

Clear pricing and infrastructure free

\$2500 per camera / year. All the footage is stored in the cloud at no additional fee and there are no hidden costs.

Protect the Whole Community

It takes all community members working together to eliminate crime, which is why we created a public-private partnership that enables businesses, neighborhoods, schools, and others to partner with your city and police department to build your network.

Learn More:



"Flock Safety continues to enhance and help our police department capture these vehicles and return the assets to their owners."

-Council member Josh McCurn of Lexington, KY



About Flock Safety ALPR

Privacy and Ethics Factsheet

How does Flock Safety keep devices and data secure?

Flock Safety holds itself to the highest level of security. We have implemented the following security policies and features:

- Flock Safety data and footage is encrypted throughout its entire lifecycle. All data is securely stored with AES256 encryption with our cloud provider, Amazon Web Services.
- On-device, data is only stored temporarily for a short time until it is uploaded to the cloud, at which point it is removed automatically from the local device. This means the data is secure from when it is on the Flock Safety device to when it is transferred to the cloud, using a secure connection to Flock Safety servers. While stored in the cloud, all data (both footage and metadata) is fully encrypted at rest.
- Flock Safety defaults to permanently deleting all data after 30 days on a rolling basis, setting a new standard in the industry.

Who has access to data collected by Flock Safety devices?

- Flock Safety's customers own 100% of their data and determine who has access. Flock Safety will never share or sell the data, per our privacy policy.
- With explicit written permission from the customer, Flock Safety does have the ability to grant law enforcement access to specific footage for a short period (24 hours, 48 hours, or however long the customer desires) in the event of an investigation following a crime. Access can only be granted through the approval of the customer.
- Flock Safety has maintenance software in place to measure device performance and image capture quality. This is used to diagnose issues preemptively and schedule service calls in the event of a device malfunction or emergency.

About Flock Safety ALPR

Privacy and Ethics Factsheet

How long does Flock Safety keep data?

- Flock Safety stores footage for only 30 days on a rolling basis by default, after which the footage is automatically hard deleted. The only exception to this is if a democratically-elected governing body or official legislates a different data retention period.

What features do Flock Safety devices have that enable audits and oversight?

- While searching for footage or other evidence on the Flock Safety platform, law enforcement agencies must enter reason codes to verify the legitimacy of the search and create an audit trail.
- Authorized users go through training to properly use our system and communicate with their dispatch teams.
- Flock Safety customers commit not to use the data collected to work with third-party repossession companies, traffic enforcement, revenue collection, unpaid fines, or towing companies. We do not use facial recognition or capture any personally identifiable information such as name, phone number, or address, and we do not work with federal government agencies for immigration enforcement purposes.
- Flock Safety's ALPR Transparency Portal, an optional free feature for all law enforcement customers, is the first public-facing dashboard for law enforcement agencies, city leaders, and local government officials to share policies, usage, and public safety outcomes related to ALPR technology. The ALPR Transparency Portal helps promote transparency and accountability in the use of policing technology in order to build community trust while creating a safer, more equitable society.

**FLOCK GROUP INC.
SERVICES AGREEMENT
ORDER FORM**

This Order Form together with the Terms (as defined herein) describe the relationship between Flock Group Inc. ("Flock") and the customer identified below ("Agency") (each of Flock and Customer, a "Party"). This order form ("Order Form") hereby incorporates and includes the "GOVERNMENT AGENCY AGREEMENT" attached (the "Terms") which describe and set forth the general legal terms governing the relationship (collectively, the "Agreement"). The Terms contain, among other things, warranty disclaimers, liability limitations and use limitations.

The Agreement will become effective when this Order Form is executed by both Parties (the "Effective Date").

Agency: CA - City of Carmel, Police Department

Legal Entity Name: City of Carmel by the Sea, a municipal corporation

Address:
4th Ave
Carmel by the Sea, California 93921

Expected Payment Method:

Contact Name: Jeff Watkins

Phone: (831) 624-6403

E-Mail: jwatkins@ci.carmel.ca.us

Billing Contact:
(if different than above)

Initial Term: 24 months

Renewal Term: 24 months

Billing Term: Billing Term: Invoice Plan payment due Net 30 per terms and conditions
Billing Frequency: 1 year invoices broken into 3 payments. 1st invoice: All professional services/implementation costs and 50% of Annual Recurring Subtotal. 2nd Invoice: 25% of Annual Recurring Subtotal. 3rd Invoice: 25% of Annual Recurring Subtotal. Annual payment at annual subscription term date invoiced for the remainder subscription term after initial 12 months.

Professional Services and One-Time Purchases

Name	Price/Usage Fee	QTY	Subtotal
Professional Services - Standard Implementation Fee	\$350.00	24.00	\$8,400.00
Professional Services - Advanced Implementation Fee	\$500.00	1.00	\$500.00

Hardware and Software Products

Annual recurring amounts over subscription term

Name	Price/Usage Fee	QTY	Subtotal
Falcon	\$2,500.00	24.00	\$60,000.00
Wing LPR	\$1,500	6.00	\$9,000.00

Subtotal Year 1:	\$77,900.00
Subscription Term:	24 Months
Annual Recurring Total:	\$69,000.00
Estimated Sales Tax:	\$0.00
Total Contract Amount:	\$146,900.00

I have reviewed and agree to the Customer Implementation Guide on Schedule B at the end of this agreement.

By executing this Order Form, Agency represents and warrants that it has read and agrees all of the terms and conditions contained in the Terms attached. The Parties have executed this Agreement as of the dates set forth below.

FLOCK GROUP, INC.

Agency: CA – City of Carmel by the Sea

By: _____

By: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date: _____

Date: _____

flock safety

GOVERNMENT AGENCY AGREEMENT

This Government Agency Agreement (this "**Agreement**") is entered into by and between Flock Group, Inc. with a place of business at 1170 Howell Mill Rd NW Suite 210, Atlanta, GA 30318 ("**Flock**") and the government agency identified in the signature block of the Order Form ("**Agency**") (each a "**Party**," and together, the "**Parties**").

RECITALS

WHEREAS, Flock offers a software and hardware situational awareness solution for automatic license plates, video and audio detection through Flock's technology platform (the "**Flock Service**"), and upon detection, the Flock Services are capable of capturing audio, video, image, and recording data and can provide notifications to Agency upon the instructions of Non-Agency End User (as defined below) ("**Notifications**").

WHEREAS, Agency desires access to the Flock Service on existing cameras, provided by Agency, or Flock provided Flock Hardware (as defined below) in order to create, view, search and archive Footage and receive Notifications, including those from Non-Agency End Users of the Flock Service (where there is an investigative or bona fide lawful purpose) such as schools, neighborhood homeowners associations, businesses, and individual users.

WHEREAS, Flock deletes all Footage on a rolling thirty (30) day basis, excluding Wing Replay which is deleted after seven (7) days. Agency is responsible for extracting, downloading and archiving Footage from the Flock System on its own storage devices for auditing for prosecutorial/administrative purposes; and

WHEREAS, Flock desires to provide Agency the Flock Service and any access thereto, subject to the terms and conditions of this Agreement, solely for the awareness, prevention, and prosecution of crime, bona fide investigations by police departments, and archiving for evidence gathering ("**Permitted Purpose**").

AGREEMENT

NOW, THEREFORE, Flock and Agency agree that this Agreement, and any addenda attached hereto or referenced herein, constitute the complete and exclusive statement of the Agreement of the Parties with respect to the subject matter of this Agreement, and replace and supersede all prior agreements, term sheets, purchase orders, correspondence, oral or written communications and negotiations by and between the Parties.

1. DEFINITIONS

Certain capitalized terms, not otherwise defined herein, have the meanings set forth or cross-referenced in this Section 1.

1.1 "**Advanced Search**" means the provision of Services, via the web interface using Flock's software applications, which utilize advanced evidence delivery capabilities including convoy analysis, multi-geo search, visual search, cradlepoint integration for automatic vehicle location, and common plate analysis.

1.2 "**Agency Data**" means the data, media and content provided by Agency through the Services. For the avoidance of doubt, the Agency Data will include the Footage.

1.3 "**Agency Generated Data**" means the messages, text, illustrations, files, images, graphics, photos, comments, sounds, music, videos, information, content, ratings, reviews, data, questions, suggestions, other information or materials posted, uploaded, displayed, published, distributed, transmitted, broadcasted, or otherwise made available on or submitted through the Wing Suite.

- 1.4. "**Agency Hardware**" means the third-party camera owned or provided by Agency and any other physical elements that interact with the Embedded Software and the Web Interface to provide the Services.
- 1.5. "**Aggregated Data**" means information that relates to a group or category of individuals, from which any potential individuals' personal identifying information has been permanently "anonymized" by commercially available standards to irreversibly alter data in such a way that a data subject (i.e., individual person or impersonal entity) can no longer be identified directly or indirectly.
- 1.6. "**Authorized End User(s)**" means any individual employees, agents, or contractors of Agency accessing or using the Services through the Web Interface, under the rights granted to Agency pursuant to this Agreement.
- 1.7. "**Deployment Plan**" means the strategic geographic mapping of the location(s) and implementation of Flock Hardware, and/or other relevant Services required under this Agreement.
- 1.8. "**Documentation**" means text and/or graphical documentation, whether in electronic or printed format, that describe the features, functions and operation of the Services which are provided by Flock to Agency in accordance with the terms of this Agreement.
- 1.9. "**Embedded Software**" means the software and/or firmware embedded or preinstalled on the Flock Hardware or Agency Hardware.
- 1.10. "**Falcon Flex**" means an infrastructure-free, location-flexible license plate reader camera that enables the Agency to self-install.
- 1.11. "**Flock Hardware**" means the Flock cameras or device, pole, clamps, solar panel, installation components, and any other physical elements that interact with the Embedded Software and the Web Interface to provide the Flock Services.
- 1.12. "**Flock IP**" means the Services, the Documentation, the Embedded Software, the Installation Services, and any and all intellectual property therein or otherwise provided to Agency and/or its Authorized End Users in connection with the foregoing.
- 1.13. "**Flock Safety Falcon™**" means an infrastructure-free license plate reader camera that utilizes Vehicle Fingerprint™ technology to capture vehicular attributes.
- 1.14. "**Flock Safety Raven™**" means an audio detection device that provides real-time alerting to law enforcement based on programmed audio events such as gunshots, breaking glass, and street racing.
- 1.15. "**Flock Safety Sparrow™**" means an infrastructure-free license plate reader camera for residential roadways that utilizes Vehicle Fingerprint™ technology to capture vehicular attributes.

- 1.17 "**Footage**" means still images, video, audio and other data captured by the Flock Hardware or Agency Hardware in the course of and provided via the Services.
- 1.18 "**Hotlist(s)**" means a digital file containing alphanumeric license plate related information pertaining to vehicles of interest, which may include stolen vehicles, stolen vehicle license plates, vehicles owned or associated with wanted or missing person(s), vehicles suspected of being involved with criminal or terrorist activities, and other legitimate law enforcement purposes. Hotlist also includes, but is not limited to, national data (i.e. NCIC) for similar categories, license plates associated with AMBER Alerts or Missing Persons/Vulnerable Adult Alerts, and includes manually entered license plate information associated with crimes that have occurred in any local jurisdiction.
- 1.19 "**Implementation Fee(s)**" means the monetary fees associated with the Installation Services, as defined below.
- 1.20 "**Installation Services**" means the services provided by Flock for installation of Agency Hardware and/or Flock Hardware, including any applicable installation of Embedded Software on Agency Hardware.
- 1.21 "**Non-Agency End User(s)**" means any individual, entity, or derivative therefrom, authorized to use the Services through the Web Interface, under the rights granted to pursuant to the terms (or to those materially similar) of this Agreement.
- 1.22 "**Services**" or "**Flock Services**" means the provision, via the Web Interface, of Flock's software applications for automatic license plate detection, alerts, audio detection, searching image records, video and sharing Footage.
- 1.23 "**Support Services**" means Monitoring Services, as defined in Section 2.10 below.
- 1.24 "**Usage Fee**" means the subscription fees to be paid by the Agency for ongoing access to Services.
- 1.25 "**Web Interface**" means the website(s) or application(s) through which Agency and its Authorized End Users can access the Services, in accordance with the terms of this Agreement.
- 1.26 "**Wing Suite**" means the Flock interface which provides real-time access to the Flock Services, location of Flock Hardware, Agency Hardware, third-party cameras, live-stream video, Wing Livestream, Wing LPR, Wing Replay, alerts and other integrations.
- 1.27 "**Wing Livestream**" means real-time video integration with third-party cameras via the Flock interface.
- 1.28 "**Wing LPR**" means software integration with third-party cameras utilizing Flock's Vehicle Fingerprint Technology™ for license plate capture.
- 1.29 "**Wing Replay**" means enhanced situational awareness encompassing Footage retention, replay ability, and downloadable content from Hot Lists integrated from third-party cameras.

1.30 "*Vehicle Fingerprint™*" means the unique vehicular attributes captured through Services such as: type, make, color, state registration, missing/covered plates, bumper stickers, decals, roof racks, and bike racks.

2. SERVICES AND SUPPORT

2.1 Provision of Access. Subject to the terms of this Agreement, Flock hereby grants to Agency a non-exclusive, non-transferable right to access the features and functions of the Services via the Web Interface during the Term, solely for the Authorized End Users. The Footage will be available for Agency's designated administrator, listed on the Order Form, and any Authorized End Users to access and download via the Web Interface for thirty (30) days. Authorized End Users will be required to sign up for an account and select a password and username ("*User ID*"). Flock will also provide Agency with the Documentation to be used in accessing and using the Services. Agency shall be responsible for all acts and omissions of Authorized End Users, and any act or omission by an Authorized End User which, if undertaken by Agency, would constitute a breach of this Agreement, shall be deemed a breach of this Agreement by Agency. Agency shall undertake reasonable efforts to make all Authorized End Users aware of the provisions of this Agreement as applicable to such Authorized End User's use of the Services and shall cause Authorized End Users to comply with such provisions. Flock may use the services of one or more third parties to deliver any part of the Services, (such as using a third party to host the Web Interface for cloud storage or a cell phone provider for wireless cellular coverage) which makes the Services available to Agency and Authorized End Users. Warranties provided by said third party service providers are the agency's sole and exclusive remedy and Flock's sole and exclusive liability with regard to such third-party services, including without limitation hosting the Web Interface. Agency agrees to comply with any acceptable use policies and other terms of any third-party service provider that are provided or otherwise made available to Agency from time to time.

2.2 Embedded Software License. Subject to all terms of this Agreement, Flock grants Agency a limited, non-exclusive, non-transferable, non-sublicensable (except to the Authorized End Users), revocable right to use the Embedded Software as installed on the Flock Hardware or Agency Hardware; in each case, solely as necessary for Agency to use the Services.

2.3 Documentation License. Subject to the terms of this Agreement, Flock hereby grants to Agency a non-exclusive, non-transferable right and license to use the Documentation during the Term in connection with its use of the Services as contemplated herein, and under Section 2.5 below.

2.4 Wing Suite License. Subject to all terms of this Agreement, Flock grants Agency a limited, non-exclusive, non-transferable, non-sublicensable (except to the Authorized End Users), revocable right to use the Wing Suite software and interface.

2.5 Usage Restrictions.

2.5.1 **Flock IP.** The permitted purpose for usage of the Flock Hardware, Agency Hardware, Documentation, Services, support, and Flock IP are solely to facilitate gathering evidence that could be used in a lawful criminal investigation by the appropriate government agency ("*Permitted Purpose*"). Agency will not, and will not permit any Authorized End Users to, (i) copy or duplicate any of the Flock IP; (ii) decompile, disassemble, reverse engineer, or otherwise attempt to obtain or perceive the source code from which any software component of any of the Flock IP is compiled or interpreted, or apply any other process or procedure to derive the source code of any software included in the Flock IP; (iii) attempt to modify, alter, tamper with or repair any of the Flock IP, or attempt to create any derivative product from any of the foregoing; (iv) interfere or attempt to interfere in any manner with the functionality or proper working of any of the Flock IP; (v) remove, obscure, or alter any notice of any intellectual property or proprietary right appearing on or contained within any of the Services or Flock IP; (vi) use the Services, support, Flock Hardware, Documentation, or the Flock IP for anything other than the Permitted Purpose; or (vii) assign, sublicense, sell, resell, lease, rent, or otherwise transfer, convey, pledge as security, or otherwise encumber, Agency's rights under Sections 2.1, 2.2, 2.3, or 2.4.

2.5.2. **Flock Hardware.** Agency understands that all Flock Hardware is owned exclusively by Flock, and that title to any Flock Hardware does not pass to Agency upon execution of this Agreement. Except for Falcon Flex products, which are designed for self-installation, Agency is not permitted to remove, reposition, re-install, tamper with, alter, adjust or otherwise take possession or control of Flock Hardware. Notwithstanding the notice and cure period set for in Section 6.3, Agency agrees and understands that in the event Agency is found to engage in any of the restricted actions of this Section 2.5.2, all warranties herein shall be null and void, and this Agreement shall be subject to immediate termination (without opportunity to cure) for material breach by Agency.

2.6 **Retained Rights; Ownership.** As between the Parties, subject to the rights granted in this Agreement, Flock and its licensors retain all right, title and interest in and to the Flock IP and its components, and Agency acknowledges that it neither owns nor acquires any additional rights in and to the foregoing not expressly granted by this Agreement. Agency further acknowledges that Flock retains the right to use the foregoing for any purpose in Flock's sole discretion. There are no implied rights.

2.7 Suspension.

2.7.1 **Service Suspension.** Notwithstanding anything to the contrary in this Agreement, Flock may temporarily suspend Agency's and any Authorized End User's access to any portion or all of the Flock IP or Flock Service if Flock reasonably determines that (a) there is a threat or attack on any of the Flock IP by Agency; (b) Agency's or any Authorized End User's use of the Flock IP disrupts or poses a security risk to the Flock IP or any other customer or vendor of Flock; (c) Agency or any Authorized End User is/are using the Flock IP for fraudulent or illegal activities; (d) Agency has violated any term of this provision, including, but not limited to, utilizing the Services for

anything other than the Permitted Purpose, or (e) any unauthorized access to Flock Services through Agency's account ("*Service Suspension*"). Agency shall not be entitled to any remedy for the Service Suspension period, including any reimbursement, tolling, or credit.

2.7.2 Service Interruption. Services may be interrupted in the event that: (a) Flock's provision of the Services to Agency or any Authorized End User is prohibited by applicable law; (b) any third-party services required for Services are interrupted; (c) if Flock reasonably believe Services are being used for malicious, unlawful, or otherwise unauthorized use; (d) there is a threat or attack on any of the Flock IP by a third party; or (e) scheduled or emergency maintenance ("*Service Interruption*"). Flock will make commercially reasonable efforts to provide written notice of any Service Interruption to Agency and to provide updates regarding resumption of access to Flock Services. Flock will use commercially reasonable efforts to resume providing access to the Services as soon as reasonably possible after the event giving rise to the Service Interruption is cured. Flock will have no liability for any damage, liabilities, losses (including any loss of data or profits), or any other consequences that Agency or any Authorized End User may incur as a result of a Service Interruption. To the extent that the Service Interruption is not caused by Agency's direct actions or by the actions of parties associated with the Agency, the expiration of the Term will be tolled by the duration of the Service Interruption (for any continuous suspension lasting at least one full day) prorated for the proportion of cameras on the Agency's account that have been impacted. For example, in the event of a Service Interruption lasting five (5) continuous days, Agency will receive a credit for five (5) free days at the end of the Term.

2.8 Installation Services.

2.8.1 Designated Locations. For installation of Flock Hardware, excluding Falcon Flex products, prior to performing the physical installation of the Flock Hardware, Flock shall advise Agency on the location and positioning of the Flock Hardware for optimal license plate image capture, as conditions and location allow. Flock may consider input from Agency regarding location, position and angle of the Flock Hardware ("*Designated Location*") and collaborate with Agency to design the Deployment Plan confirming the Designated Locations. Flock shall have final discretion on location of Flock Hardware. Flock shall have no liability to Agency resulting from any poor performance, functionality or Footage resulting from or otherwise relating to the Designated Locations or delay in installation due to Agency's delay in confirming Designated Locations, in ordering and/or having the Designated Location ready for installation including having all electrical work preinstalled and permits ready, if necessary. After installation, any subsequent changes to the Deployment Plan ("*Reinstalls*") will incur a charge for Flock's then-current list price for Reinstalls, as listed in the then-current Reinstall policy (available at <https://www.flocksafety.com/reinstall-fee-schedule>) and any equipment fees. For clarity, Agency will receive prior notice and provide approval for any such fees. These changes include but are not limited to re-positioning, adjusting of the mounting, re-angling, removing foliage, replacement, changes to heights of poles, regardless of whether the need for Reinstalls related to vandalism, weather, theft, lack of criminal activity in view, and the like. Flock shall have full discretion on decision to reinstall Flock Hardware.

2.8.2 **Agency Installation Obligations.** Agency agrees to allow Flock and its agents reasonable access in and near the Designated Locations at all reasonable times upon reasonable notice for the purpose of performing the installation work. Although Flock Hardware is designed to utilize solar power, certain Designated Locations may require a reliable source of 120V or 240V AC power. In the event adequate solar power is not available, Agency is solely responsible for costs associated with providing a reliable source of 120V or 240V AC power to Flock Hardware. Flock will provide solar options to supply power at each Designated Location. If Agency refuses recommended solar options, Agency waives any reimbursement, tolling, or credit for any suspension period of Flock Services due to low solar power. Additionally, Agency is solely responsible for (i) any permits or associated costs, and managing the permitting process of installation of cameras or AC power; (ii) any federal, state, or local taxes including property, license, privilege, sales, use, excise, gross receipts, or other similar taxes which may now or hereafter become applicable to, measured by or imposed upon or with respect to the installation of the Flock Hardware, its use (excluding tax exempt entities), or (iii) any other supplementary cost for services performed in connection with installation of the Flock Hardware, including but not limited to contractor licensing, engineered drawings, rental of specialized equipment, or vehicles, third-party personnel (i.e. Traffic Control Officers, Electricians, State DOT-approved poles, etc., if necessary), such costs to be approved by the Agency ("**Agency Installation Obligations**"). In the event that a Designated Location for Flock Hardware requires permits, Flock may provide the Agency with a temporary alternate location for installation pending the permitting process. Once the required permits are obtained, Flock will relocate the Flock Hardware from the temporary alternate location to the permitted location at no additional cost. Without being obligated or taking any responsibility for the foregoing, Flock may pay and invoice related costs to Agency if Agency did not address them prior to the execution of this Agreement or a third party requires Flock to pay. Agency represents and warrants that it has, or shall lawfully obtain, all necessary right title and authority and hereby authorizes Flock to install the Flock Hardware at the Designated Locations and to make any necessary inspections or tests in connection with such installation.

2.8.3 **Flock's Obligations.** Installation of Flock Hardware shall be installed in a workmanlike manner in accordance with Flock's standard installation procedures, and the installation will be completed within a reasonable time from the time that the Designated Locations are confirmed. Upon removal of Flock Hardware, Flock shall restore the location to its original condition, ordinary wear and tear excepted. Following the initial installation of the Flock Hardware and any subsequent Reinstalls or maintenance operations, Flock's obligation to perform installation work shall cease; however, for the sole purpose of validating installation, Flock will continue to monitor the performance of Flock Hardware for the length of the Term and will receive access to the Footage for a period of seven (7) business days after the initial installation for quality control and provide any necessary maintenance. Labor may be provided by Flock or a third-party. Flock is not obligated to install, reinstall, or provide physical maintenance to Agency Hardware. Notwithstanding anything to the contrary, Agency understands that Flock will not provide installation services for Falcon Flex products.

2.8.4 **Ownership of Hardware.** Flock Hardware shall remain the personal property of Flock and will be removed upon the natural expiration of this Agreement at no additional cost to Agency. Agency shall not perform any acts which would interfere with the retention of title of the Flock Hardware by Flock. Should Agency default on any

payment of the Flock Services, Flock may remove Flock Hardware at Flock's discretion. Such removal, if made by Flock, shall not be deemed a waiver of Flock's rights to any damages Flock may sustain as a result of Agency's default and Flock shall have the right to enforce any other legal remedy or right.

2.9 Hazardous Conditions. Unless otherwise stated in the Agreement, Flock's price for its services under this Agreement does not contemplate work in any areas that contain hazardous materials, or other hazardous conditions, including, without limit, asbestos, lead, toxic or flammable substances. In the event any such hazardous materials are discovered in the designated locations in which Flock is to perform services under this Agreement, Flock shall have the right to cease work immediately in the area affected until such materials are removed or rendered harmless.

2.10 Support Services. Subject to the payment of fees, Flock shall monitor the performance and functionality of Flock Services and may, from time to time, advise Agency on changes to the Flock Services, Installation Services, or the Designated Locations which may improve the performance or functionality of the Services or may improve the quality of the Footage. The work, its timing, and the fees payable relating to such work shall be agreed by the Parties prior to any alterations to or changes of the Services or the Designated Locations ("**Monitoring Services**"). Flock will use commercially reasonable efforts to respond to requests for support. Flock will provide Agency with reasonable technical and on-site support and maintenance services ("**On-Site Services**") in-person or by email at support@flocksafety.com, at no additional cost. Notwithstanding anything to the contrary, Agency is solely responsible for installation of Falcon Flex products. Agency further understands and agrees that Flock will not provide monitoring services or on-site services for Falcon Flex.

2.11 Special Terms. From time to time, Flock may offer certain special terms related to guarantees, service and support which are indicated in the proposal and on the Order Form and will become part of this Agreement, upon Agency's prior written consent ("**Special Terms**"). To the extent that any terms of this Agreement are inconsistent or conflict with the Special Terms, the Special Terms shall control.

2.12 Upgrades to Platform. Flock may, in its sole discretion, make any upgrades to system or platform that it deems necessary or useful to (i) maintain or enhance (a) the quality or delivery of Flock's products or services to its agencies, (b) the competitive strength of, or market for, Flock's products or services, (c) such platform or system's cost efficiency or performance, or (ii) to comply with applicable law. Parties understand that such upgrades are necessary from time to time and will not materially change any terms or conditions within this Agreement.

3. RESTRICTIONS AND RESPONSIBILITIES

3.1 Agency Obligations. Flock will assist Agency Authorized End Users in the creation of a User ID. Agency agrees to provide Flock with accurate, complete, and updated registration information. Agency may not select as its User ID a name that Agency does not have the right to use, or another person's name with the intent to impersonate that person. Agency may not transfer its account to anyone else without prior written permission of Flock. Agency

will not share its account or password with anyone and must protect the security of its account and password. Unless otherwise stated and defined in this Agreement, Agency may not designate Authorized End Users for persons who are not officers, employees, or agents of Agency. Authorized End Users shall only use Agency-issued email addresses for the creation of their User ID. Agency is responsible for any activity associated with its account. Agency shall be responsible for obtaining and maintaining any equipment and ancillary services needed to connect to, access or otherwise use the Services. Agency will, at its own expense, provide assistance to Flock, including, but not limited to, by means of access to, and use of, Agency facilities, as well as by means of assistance from Agency personnel to the limited extent any of the foregoing may be reasonably necessary to enable Flock to perform its obligations hereunder, including, without limitation, any obligations with respect to Support Services or any Installation Services.

3.2 Agency Representations and Warranties. Agency represents, covenants, and warrants that Agency will use the Services only in compliance with this Agreement and all applicable laws and regulations, including but not limited to any laws relating to the recording or sharing of video, photo, or audio content. Although Flock has no obligation to monitor Agency 's use of the Services, Flock may do so and may prohibit any use of the Services it believes may be (or alleged to be) in violation of the foregoing.

4. CONFIDENTIALITY: AGENCY DATA

4.1 Confidentiality. To the extent allowable by applicable FOIA and state-specific Public Records Acts, each Party (the "**Receiving Party**") understands that the other Party (the "**Disclosing Party**") has disclosed or may disclose business, technical or financial information relating to the Disclosing Party's business (hereinafter referred to as "**Proprietary Information**" of the Disclosing Party). Proprietary Information of Flock includes non-public information regarding features, functionality and performance of the Services. Proprietary Information of Agency includes non-public data provided by Agency to Flock or collected by Flock via the Flock Hardware or Agency Hardware, to enable the provision of the Services, which includes but is not limited to geolocation information and environmental data collected by sensors. The Receiving Party agrees: (i) to take the same security precautions to protect against disclosure or unauthorized use of such Proprietary Information that the Party takes with its own proprietary information, but in no event will a Party apply less than reasonable precautions to protect such Proprietary Information, and (ii) not to use (except in performance of the Services or as otherwise permitted herein) or divulge to any third person any such Proprietary Information. Flock's use of the Proprietary Information may include processing the Proprietary Information to send Agency alerts, or to analyze the data collected to identify motion or other events. The Disclosing Party agrees that the foregoing shall not apply with respect to any information that the Receiving Party can document (a) is or becomes generally available to the public, or (b) was in its possession or known by it prior to receipt from the Disclosing Party, or (c) was rightfully disclosed to it without restriction by a third party, or (d) was independently developed without use of any Proprietary Information of the Disclosing Party. Nothing in this Agreement will prevent the Receiving Party from disclosing the Proprietary Information pursuant to any judicial or governmental order, provided that the Receiving Party gives the Disclosing

Party reasonable prior notice of such disclosure to contest such order. For clarity, Flock may access, use, preserve and/or disclose the Footage to law enforcement authorities, government officials, and or third parties, if legally required to do so or if Flock has a good faith belief that such access, use, preservation or disclosure is reasonably necessary to: (a) comply with a legal process or request; (b) enforce this Agreement, including investigation of any potential violation thereof; (c) detect, prevent or otherwise address security, fraud or technical issues; or (d) protect the rights, property or safety of Flock, its users, a third party, or the public as required or permitted by law, including respond to an emergency situation. Flock may store deleted Footage in order to comply with certain legal obligations, but such retained Footage will not be retrievable without a valid court order.

4.2 Agency Data. As between Flock and Agency, all right, title and interest in the Agency Data, belong to and are retained solely by Agency. Agency hereby grants to Flock a limited, non-exclusive, royalty-free, worldwide license to (i) use the Agency Data and perform all acts with respect to the Agency Data as may be necessary for Flock to provide the Flock Services to Agency, including without limitation the Support Services set forth in Section 2.10 above, and a non-exclusive, perpetual, irrevocable, worldwide, royalty-free, fully paid license to use, reproduce, modify, display, and distribute the Agency Data as a part of the Aggregated Data, (ii) disclose the Agency Data (both inclusive of any Footage) to enable law enforcement monitoring for elected law enforcement Hotlists as well as provide Footage search access to law enforcement for investigative purposes only, and (iii) and obtain Aggregated Data as set forth below in Section 4.5. As between Agency and Non-Agency End Users that have prescribed access of Footage to Agency, each of Agency and Non-Agency End Users will share all right, title and interest in the Non-Agency End User Data. This Agreement does not by itself make any Non-Agency End User Data the sole property or the Proprietary Information of Agency. Flock will automatically delete Footage older than thirty (30) days. Agency has a thirty (30) day window to view, save and/or transmit Footage to the relevant government agency prior to its deletion. Notwithstanding the foregoing, Flock automatically deletes Wing Replay after seven (7) days, during which time Agency may view, save and/or transmit such data to the relevant government agency prior to deletion. Flock does not own and shall not sell Agency Data.

4.3 Agency Generated Data in Wing Suite. Parties understand that Flock does not own any right, title, or interest to third-party video integrated into the Wing Suite. Flock may provide Agency with the opportunity to post, upload, display, publish, distribute, transmit, broadcast, or otherwise make available on or submit through the Wing Suite, messages, text, illustrations, files, images, graphics, photos, comments, sounds, music, videos, information, content, ratings, reviews, data, questions, suggestions, or other information or materials produced by Agency. Agency shall retain whatever legally cognizable right, title, and interest that Agency has in Agency Generated Data. Agency understands and acknowledges that Flock has no obligation to monitor or enforce Agency's intellectual property rights to Agency Generated Data. To the extent legally permissible, Agency grants Flock a non-exclusive, perpetual, irrevocable, worldwide, royalty-free, fully paid license to use, reproduce, modify, display, and distribute the Agency Generated Data for the sole purpose of providing Flock Services. Flock does not own and shall not sell Agency Generated Data.

4.4 Feedback. If Agency provides any suggestions, ideas, enhancement requests, feedback, recommendations or other information relating to the subject matter hereunder, Agency hereby assigns (and will cause its agents and representatives to assign) to Flock all right, title and interest (including intellectual property rights) with respect to or resulting from any of the foregoing.

4.5 Aggregated Data. Flock shall have the right to collect, analyze, and anonymize Agency Data and Agency Generated Data to create Aggregated Data to use and perform the Services and related systems and technologies, including the training of machine learning algorithms. Agency hereby grants Flock a non-exclusive, worldwide, perpetual, royalty-free right (during and after the Term hereof) to use and distribute such Aggregated Data to improve and enhance the Services and for other development, diagnostic and corrective purposes, other Flock offerings, and crime prevention efforts. Parties understand that the aforementioned license is required for continuity of Services. No rights or licenses are granted except as expressly set forth herein. Flock does not sell Aggregated Data

5. PAYMENT OF FEES

5.1.1 Software Product Fees. For Order Forms listing Wing Suite, Advanced Search and other software-only products, Agency will pay Flock the fees for the Initial Term (as described on the Order Form attached hereto) on or before the 30th day from the date of invoice. For any Renewal Terms, Agency shall pay invoice on or before the 30th day from the date of renewal invoice.

5.1.2 Hardware Product Fees. For Order Forms listing Falcon, Sparrow, Raven and Falcon Flex products, Agency will pay Flock fifty percent (50%) of the fees for the Initial Term as set forth on the Order Form on or before the 30th day from date of invoice. Upon commencement of installation, Flock will issue an invoice for twenty-five percent (25%) of total fees, and Agency shall pay on or before 30th day following date of invoice. Upon completion of installation, Flock will issue an invoice for the remaining balance and Agency shall pay on or before 30th day following date of final invoice. Flock is not obligated to commence the Installation Services unless and until the first payment has been made and shall have no liability resulting from any delay related thereto. For any Renewal Terms, Agency shall pay the total invoice on or before the 30th day from the date of renewal invoice.

5.2 Notice of Changes to Fees. Flock reserves the right to change the fees or applicable charges and to institute new charges and fees on subsequent terms by providing sixty (60) days' notice prior to the end of such Initial Term or Renewal Term (as applicable) to Agency (which may be sent by email).

5.3 Invoicing, Late Fees; Taxes. Flock may choose to bill through an invoice, in which case, full payment for invoices must be received by Flock thirty (30) days after the receipt of invoice. If Agency is a non-tax-exempt entity, Agency shall be responsible for all taxes associated with Services other than U.S. taxes based on Flock's net income. If Agency believes that Flock has billed Agency incorrectly, Agency must contact Flock no later than sixty (60) days after the closing date on the first billing statement in which the error or problem appeared, in order to

receive an adjustment or credit. Agency acknowledges and agrees that a failure to contact Flock within this sixty (60) day period will serve as a waiver of any claim Agency may have had as a result of such billing error.

6. TERM AND TERMINATION

6.1 Term. The initial term of this Agreement shall be for the period of time set forth on the Order Form and shall commence at the time outlined in this section below (the "**Term**"). Following the Term, unless otherwise indicated on the Order Form, this Agreement will automatically renew for successive renewal terms of the greater of one year or the length set forth on the Order Form (each, a "**Renewal Term**") unless either Party gives the other Party notice of non-renewal at least thirty (30) days prior to the end of the then-current term.

- a. For Wing Suite products: the Term shall commence upon execution of this Agreement and continue for one (1) year, after which, the Term may be extended by mutual consent of the Parties, unless terminated by either Party.
- b. For Falcon and Sparrow products: the Term shall commence upon first installation and validation of Flock Hardware.
- c. For Raven products: the Term shall commence upon first installation and validation of Flock Hardware.
- d. For Falcon Flex products: the Term shall commence upon execution of this Agreement.
- e. For Advanced Search products: the Term shall commence upon execution of this Agreement.

6.2 Termination for Convenience. At any time during the agreed upon Term, either Party may terminate this Agreement for convenience. Termination for convenience of the Agreement by the Agency will be effective immediately. Termination for convenience by Agency will result in a one-time removal fee of \$500 per Flock Hardware. Termination for convenience by Flock will not result in any removal fees. Upon termination for convenience, a refund will be provided for Flock Hardware, prorated for any fees for the remaining Term length set forth previously. Wing Suite products and Advanced Search are not subject to refund for early termination. Flock will provide advanced written notice and remove all Flock Hardware at Flock's own convenience, within a commercially reasonable period of time upon termination. Agency's termination of this Agreement for Flock's material breach of this Agreement shall not be considered a termination for convenience for the purposes of this Section 6.2.

6.3 Termination. Notwithstanding the termination provisions in Section 2.5.2, in the event of any material breach of this Agreement, the non-breaching Party may terminate this Agreement prior to the end of the Term by giving thirty (30) days prior written notice to the breaching Party; provided, however, that this Agreement will not terminate if the breaching Party has cured the breach prior to the expiration of such thirty (30) day period. Either Party may terminate this Agreement, without notice, (i) upon the institution by or against the other Party of insolvency, receivership or bankruptcy proceedings, (ii) upon the other Party's making an assignment for the benefit of creditors, or (iii) upon the other Party's dissolution or ceasing to do business. Upon termination for Flock's material breach, Flock will refund to Agency a pro-rata portion of the pre-paid fees for Services not received due to such termination.

6.4 **No-Fee Term.** Flock will provide Agency with complimentary access to Hotlist alerts, as further described in Section 4.2 ("**No-Fee Term**"). In the event a Non-Agency End User grants Agency access to Footage and/or notifications from a Non-Agency End User, Agency will have access to Non-Agency End User Footage and/or notifications until deletion, subject to a thirty (30) day retention policy for all products except Wing Replay, which is subject to a seven (7) day retention policy. Flock may, in their sole discretion, provide access or immediately terminate the No-Fee Term. The No-Fee Term will survive the Term of this Agreement. Flock, in its sole discretion, can determine to impose a price per No-Fee Term upon thirty (30) days' notice to Agency. Agency may terminate any No-Fee Term or access to future No-Fee Terms upon thirty (30) days' notice.

6.5 **Survival.** The following Sections will survive termination: 2.5, 2.6, 3, 4, 5, 6.4, 7.3, 7.4, 8.1, 8.2, 8.3, 10.1 and 10.6

7. REMEDY; WARRANTY AND DISCLAIMER

7.1 **Remedy.** Upon a malfunction or failure of Flock Hardware or Embedded Software (a "**Defect**"), Agency must notify Flock's technical support as described in Section 2.10 above. If Flock is unable to correct the Defect, Flock shall, or shall instruct one of its contractors to repair or replace the Flock Hardware or Embedded Software suffering from the Defect. Flock reserves the right in their sole discretion to refuse or delay replacement or its choice of remedy for a Defect until after it has inspected and tested the affected Flock Hardware provided that such inspection and test shall occur within a commercially reasonable time, but no longer than seven (7) business days after Agency notifies the Flock of a known Defect. In the event of a Defect, Flock will repair or replace the defective Flock Hardware at no additional cost to Agency. Absent a Defect, in the event that Flock Hardware is lost, stolen, or damaged, Agency may request that Flock replace the Flock Hardware at a fee according to the then-current Reinstall policy (<https://www.flocksafety.com/reinstall-fee-schedule>). Agency shall not be required to replace subsequently lost, damaged or stolen Flock Hardware, however, Agency understands and agrees that functionality, including Footage, will be materially affected due to such subsequently lost, damaged or stolen Flock Hardware and that Flock will have no liability to Agency regarding such affected functionality nor shall the Usage Fee or Implementation Fees owed be impacted. Flock is under no obligation to replace or repair Flock Hardware or Agency Hardware.

7.2 **Exclusions.** Flock will not provide the remedy described in Section 7.1 if Agency has misused the Flock Hardware, Agency Hardware, or Service in any manner.

7.3 **Warranty.** Flock shall use reasonable efforts consistent with prevailing industry standards to maintain the Services in a manner which minimizes errors and interruptions in the Services and shall perform the Installation Services in a professional and workmanlike manner. Services may be temporarily unavailable for scheduled maintenance or for unscheduled emergency maintenance, either by Flock or by third-party providers, or because of

other causes beyond Flock's reasonable control, but Flock shall use reasonable efforts to provide advance notice in writing or by e-mail of any scheduled service disruption.

7.4 Disclaimer. THE REMEDY DESCRIBED IN SECTION 7.1 ABOVE IS AGENCY'S SOLE REMEDY, AND FLOCK'S SOLE LIABILITY, WITH RESPECT TO DEFECTIVE EMBEDDED SOFTWARE. FLOCK DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED OR ERROR FREE; NOR DOES IT MAKE ANY WARRANTY AS TO THE RESULTS THAT MAY BE OBTAINED FROM USE OF THE SERVICES. EXCEPT AS EXPRESSLY SET FORTH IN THIS SECTION, THE SERVICES ARE PROVIDED "AS IS" AND FLOCK DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. THIS DISCLAIMER OF SECTION 7.4 ONLY APPLIES TO THE EXTENT ALLOWED BY THE GOVERNING LAW OF THE STATE MENTIONED IN SECTION 10.6.

7.5 Insurance. Flock will maintain commercial general liability policies with policy limits reasonably commensurate with the magnitude of Flock's business risk. Certificates of Insurance can be provided upon request.

7.6 Force Majeure. Parties are not responsible or liable for any delays or failures in performance from any cause beyond their control, including, but not limited to acts of God, changes to law or regulations, embargoes, war, terrorist acts, acts or omissions of third-Party technology providers, riots, fires, earthquakes, floods, power blackouts, strikes, supply chain shortages of equipment or supplies, weather conditions or acts of hackers, internet service providers or any other third Party acts or omissions. Force Majeure includes the novel coronavirus Covid-19 pandemic, and the potential spread of variants, which is ongoing as of the date of the execution of this Agreement.

8. LIMITATION OF LIABILITY; NO FEE TERM; INDEMNITY

8.1 Limitation of Liability. NOTWITHSTANDING ANYTHING TO THE CONTRARY, FLOCK AND ITS SUPPLIERS (INCLUDING BUT NOT LIMITED TO ALL HARDWARE AND TECHNOLOGY SUPPLIERS), OFFICERS, AFFILIATES, REPRESENTATIVES, CONTRACTORS AND EMPLOYEES SHALL NOT BE RESPONSIBLE OR LIABLE WITH RESPECT TO ANY SUBJECT MATTER OF THIS AGREEMENT OR TERMS AND CONDITIONS RELATED THERETO UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY, PRODUCT LIABILITY, OR OTHER THEORY: (A) FOR ERROR OR INTERRUPTION OF USE OR FOR LOSS OR INACCURACY, INCOMPLETENESS OR CORRUPTION OF DATA OR FOOTAGE OR COST OF PROCUREMENT OF SUBSTITUTE GOODS, SERVICES OR TECHNOLOGY OR LOSS OF BUSINESS; (B) FOR ANY INDIRECT, EXEMPLARY, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES; (C) FOR ANY MATTER BEYOND FLOCK'S ACTUAL KNOWLEDGE OR REASONABLE CONTROL INCLUDING REPEAT CRIMINAL ACTIVITY OR INABILITY TO CAPTURE FOOTAGE OR IDENTIFY AND/OR CORRELATE A LICENSE PLATE WITH THE FBI DATABASE; (D) FOR ANY PUBLIC DISCLOSURE OF PROPRIETARY INFORMATION MADE IN GOOD FAITH; (E) FOR CRIME PREVENTION; OR (F) FOR ANY AMOUNTS THAT, TOGETHER WITH AMOUNTS ASSOCIATED WITH

ALL OTHER CLAIMS, EXCEED THE FEES PAID AND/OR PAYABLE BY AGENCY TO FLOCK FOR THE SERVICES UNDER THIS AGREEMENT IN THE TWELVE (12) MONTHS PRIOR TO THE ACT OR OMISSION THAT GAVE RISE TO THE LIABILITY, IN EACH CASE, WHETHER OR NOT FLOCK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY OF SECTION 8 ONLY APPLIES TO THE EXTENT ALLOWED BY THE GOVERNING LAW OF THE STATE MENTIONED IN SECTION 10.6.

8.2 Additional No-Fee Term Requirements. IN NO EVENT SHALL FLOCK'S AGGREGATE LIABILITY, IF ANY, ARISING OUT OF OR IN ANY WAY RELATED TO THE COMPLIMENTARY NO-FEE TERM AS DESCRIBED IN SECTION 6.4 EXCEED \$100, WITHOUT REGARD TO WHETHER SUCH CLAIM IS BASED IN CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE. Parties acknowledge and agree that the essential purpose of this Section 8.2 is to allocate the risks under the No-Fee Term described in Section 6.4 and limit potential liability given the aforementioned complimentary service, which would have been substantially higher if Flock were to assume any further liability other than as set forth herein. Flock has relied on these limitations in determining whether to provide the complementary No-Fee Term. The limitations set forth in this Section 8.2 shall not apply to claims or damages resulting from Flock's other obligations under this Agreement.

8.3 Responsibility. Each Party to this Agreement shall assume the responsibility and liability for the acts and omissions of its own employees, deputies, officers, or agents, in connection with the performance of their official duties under this Agreement. Each Party to this Agreement shall be liable (if at all) only for the torts of its own officers, agents, or employees.

9. INDEMNIFICATION

Agency hereby agrees to indemnify and hold harmless Flock against any damages, losses, liabilities, settlements and expenses in connection with any claim or action that arises from an alleged violation of Section 3.1, a breach of this Agreement, Agency's Installation Obligations, Agency's sharing of any data in connection with the Flock system, Flock employees or agent or Non-Agency End Users, or otherwise from Agency's use of the Services, Flock Hardware, Agency Hardware and any Embedded Software, including any claim that such actions violate any applicable law or third Party right. Although Flock has no obligation to monitor Agency's use of the Services, Flock may do so and may prohibit any use of the Services it believes may be (or alleged to be) in violation of Section 3.1 or this Agreement.

Flock agrees to indemnify and hold Agency harmless against any damages, losses, liabilities, settlements and expenses, including attorney's fees and costs arising out of third party claims for copyright and intellectual property infringement, public records act claims, an alleged violation of Flock's obligations under this agreement, Flock's

sharing of any data in connection with the Flock system. Flock employees or agent or Non-Agency End Users, or otherwise from Flock's provision of Services, Flock Hardware, Agency Hardware and any Embedded Software, including any claim that such actions violate any applicable law or third Party right.

10. MISCELLANEOUS

10.1 Compliance With Laws. The Agency and Flock and its agents agree to comply with all applicable local, state and federal laws, regulations, policies and ordinances and their associated record retention schedules, including responding to any subpoena request(s). In the event Flock is legally compelled to comply with a judicial order, subpoena, or government mandate, to disclose Agency Data or Agency Generated Data, Flock will provide Agency with notice.

10.2 Severability. If any provision of this Agreement is found to be unenforceable or invalid, that provision will be limited or eliminated to the minimum extent necessary so that this Agreement will otherwise remain in full force and effect.

10.3 Assignment. This Agreement is not assignable, transferable or sublicensable by either Party, without prior consent. Notwithstanding the foregoing, either Party may assign this Agreement, without the other Party's consent, (i) to any parent, subsidiary, or affiliate entity, or (ii) to any purchaser of all or substantially all of such Party's assets or to any successor by way of merger, consolidation or similar transaction.

10.4 Entire Agreement. This Agreement, together with the Order Form(s), the then-current Reinstall policy (<https://www.flocksafety.com/reinstall-fee-schedule>), Deployment Plan(s), and any attached addenda are the complete and exclusive statement of the mutual understanding of the Parties and supersedes and cancels all previous written and oral agreements, communications and other understandings relating to the subject matter of this Agreement, and that all waivers and modifications must be in a writing signed by both Parties, except as otherwise provided herein. None of Agency's purchase orders, authorizations or similar documents will alter the terms of this Agreement, and any such conflicting terms are expressly rejected. In the event of any conflict of terms found in this Agreement or any other terms and conditions, the terms of this Agreement shall prevail.

10.5 Relationship. No agency, partnership, joint venture, or employment is created as a result of this Agreement and Agency does not have any authority of any kind to bind Flock in any respect whatsoever. Flock shall at all times be and act as an independent contractor.

10.6 Governing Law; Venue. This Agreement shall be governed by the laws of the State in which the Agency is located. The Parties hereto agree that venue would be proper in the chosen courts of the State of which the Agency is located. The Parties agree that the United Nations Convention for the International Sale of Goods is excluded in its entirety from this Agreement.

10.7 **Publicity.** Upon prior consent from Agency, Flock has the right to reference and use Agency's name and trademarks and disclose the nature of the Services provided hereunder in each case in business and development and marketing efforts, including without limitation on Flock's website.

10.8 **Export.** Agency may not remove or export from the United States or allow the export or re-export of the Flock IP or anything related thereto, or any direct product thereof in violation of any restrictions, laws or regulations of the United States Department of Commerce, the United States Department of Treasury Office of Foreign Assets Control, or any other United States or foreign agency or authority. As defined in Federal Acquisition Regulation ("FAR"), section 2.101, the Services, the Flock Hardware and Documentation are "commercial items" and according to the Department of Defense Federal Acquisition Regulation ("DFAR") section 252.2277014(a)(1) and are deemed to be "commercial computer software" and "commercial computer software documentation." Flock is compliant with FAR Section 889 and does not contract or do business with, use any equipment, system, or service that uses the enumerated banned Chinese telecommunication companies, equipment or services as a substantial or essential component of any system, or as critical technology as part of any Flock system. Consistent with DFAR section 227.7202 and FAR section 12.212, any use, modification, reproduction, release, performance, display, or disclosure of such commercial software or commercial software documentation by the U.S. Government will be governed solely by the terms of this Agreement and will be prohibited except to the extent expressly permitted by the terms of this Agreement.

10.9 **Headings.** The headings are merely for organization and should not be construed as adding meaning to the Agreement or interpreting the associated sections.

10.10 **Authority.** Each of the below signers of this Agreement represent that they understand this Agreement and have the authority to sign on behalf of and bind the Parties they are representing.

10.11 **Notices.** All notices under this Agreement will be in writing and will be deemed to have been duly given when received, if personally delivered; when receipt is electronically confirmed, if transmitted by email; the day after it is sent, if sent for next day delivery by recognized overnight delivery service; and upon receipt, if sent by certified or registered mail, return receipt requested.

FLOCK NOTICES ADDRESS:

1170 HOWELL MILL ROAD, NW SUITE 210
ATLANTA, GA 30318
ATTN: LEGAL DEPARTMENT
EMAIL: legal@flocksafety.com

AGENCY NOTICES ADDRESS:

ADDRESS:

City of Carmel City Hall
4th Ave

Carmel, California 93921

ATTN:
EMAIL:

Flock Camera Questions: from previous Ad Hoc Committee Meetings:**Yellow: From June 10th Meeting**

1. **Can we place the cameras on existing PG& E Light Poles, Power Poles-** Yes- With Approval from PG& E we can hardwire the cameras and mount them on existing power poles and light poles. We did this with our existing cameras (2017)
2. **Do we need cameras in the residential area?** Comments from the group were to remove them from RA.- Cameras can be placed where they are needed, That would be a council decision.
3. **No Black Poles- Could these be wood?-** Yes, the poles could be wood.
4. **Can we use something other than Cloud based storage?-** Not with the Flock system.
5. **Can people opt out of the camera system? Would that be just our system or all?-** Flock offers an Opt out service and it would be for our system only. This is used for HOA's but something we could explore for the community. Yes, it would be our system only.
6. **Can cameras be installed on Buildings?-** Yes, but these cameras need to be placed in an area where they can view license plates. On buildings the view may be blocked or angle may not right.
7. **Can you provide a policing strategy (Point of View) for locations?** - Yes, this would be an import reason for the placement of cameras. We want to optimize safety and their use given the cost.
8. **Have we looked at competitors of Flock?-** I am unsure if the previous Chief's have looked at competitors. I am convinced that Flock is the leader in camera deployment for law enforcement. Flock is used by most agencies and all agencies in our area. We are increasing our ability to prevent and solve crime by using Flock cameras. Sharing information via Flock also provides increased chances in locating lost or missing persons.
9. **How many Cameras do we need?** That is a decision that needs to be made and impacts the effectiveness of the system. Wha the balance the community is looking for?
10. **Can we put them only on the perimeter, like our existing cameras?-** Yes, we already have placed them on the perimeter.
11. **What is the need/advantage of having them downtown?-** We create a double layer of safety. When investigating a crime multiple cameras can help us confirm the location, route of a suspected vehicle and help solidify a case for further investigation (if needed).