





Memorandum

TO: Kevin J. Jackson, Village Manager 

FROM: Shatonya Johnson, Interim Chief of Police 

FOR: Village President and Board of Trustees

DATE: August 3, 2022

SUBJECT: Flock Safety ALPR Implementation Status

The purpose of this memorandum is to update the Village Board on the implementation status of Flock Safety Automated License Plate Reader (ALPR) technology including the results of community engagement with and input from the Civic Information System Commission (CISC) and Citizen Police Oversight Committee (CPOC).

Background

On April 4, 2022, the Village Board approved an Agreement with Flock Safety for the implementation of ALPR technology with eight cameras and directed the Police Department to engage with CISC and CPOC to review the Police Department's draft General Order/operational policy on Flock Safety ALPR technology regarding data privacy and accountability, respectively. After meeting with both commissions, the Police Department has finalized its General Order/operational policy with appropriate privacy protections and accountability measures that will enable responsible and effective implementation of Flock Safety ALPR technology.

Training for all Department personnel authorized to use Flock Safety ALPR technology has been completed. Staff has developed a webpage that will be accessible to the public at www.oak-park.us/alpr. The webpage includes information on how the technology works, frequently asked questions, the governing policy, and will include any reports produced relating to Flock Safety ALPR implementation. Additionally, the webpage includes a link to our transparency portal which will provide the public with access to statistical information on the use of Flock Safety ALPR technology. Implementation of Flock Safety ALPR technology will occur on, Thursday, August 4, 2022.

Commission Engagement Meetings

On May 12, 2022, the Police Department met with CISC and on May 25, 2022, met with CPOC. CISC and CPOC received copies of the draft General Order/operational policy and a memorandum. During the meetings, the Police Department provided an overview of the draft General Order/operational policy and answered questions related to safeguarding data and police accountability.

Flock Safety ALPR Implementation Status

August 3, 2022

Page 2

CISC and CPOC offered recommendations from various perspectives and were encouraged to forward any additional questions and recommendations via email. CISC and CPOC sent follow-up questions and recommendations to the Police Department for review. The Police Department responded to all questions and recommendations. Recommendations were thoughtfully considered in relation to operational feasibility. Several recommendations were included in the final General Order and the Police Department offered an explanation for any that could not be feasibly included. Attached are the questions and recommendations from CISC and CPOC with the Police Department responses to each.

Four common issues emerged in the recommendations from both commissions: (1) The use of the cameras for very specific crimes: stolen vehicles and violent crimes; (2) The ability to FOIA data in Flock Technology; (3) Granting access to only the partnering agencies that share our values; and (4) CPOC should be able to monitor partnering agencies access to OPPD's camera data. Each of these concerns were addressed in the General Order and explained in the attached responses.

If you have any questions, please contact Shatonya Johnson, Interim Chief of Police, at (708) 358-5504 or sjohnson@oak-park.us.

Attachments:

1. ALPR General Order
2. Map of ALPR Locations
3. Response to the Four Common Issues
4. Response to CISC's Recommendations (Combined Ptacek & Wesley)
5. Response to CPOC's Recommendations
6. Response to CPOC's Questions (Combined Powers & Wright)

cc: Civic Information Systems Commission
Citizens Police Oversight Committee
Lisa Shelley, Deputy Village Manager
Ahmad Zayyad, Deputy Village Manager
Christina M. Waters, Village Clerk
All Department Directors



OAK PARK POLICE DEPARTMENT
GENERAL ORDER



police@oak-park.us

www.oak-park.us/police

708-386-3800

DATE OF ISSUE 01 AUGUST 22	EFFECTIVE DATE 03 AUGUST 22	DISTRIBUTION C	NUMBER 4.68
SUBJECT AUTOMATED LICENSE PLATE READER (ALPR)			
RELATED DIRECTIVES	RE-EVALUATION DATE	ADDENDUM 1	
AMENDS	RESCINDS	NO. PAGES 6	

I. PURPOSE:

Automated License Plate Reader (ALPR) technology, also known as License Plate Recognition, provides automated detection of license plates. ALPRs are used by the Oak Park Police Department (OPPD) to convert data associated with vehicle license plates for official law enforcement purposes as defined for purposes of this General Order, including identifying stolen or wanted vehicles, stolen license plates and missing persons.

II. POLICY:

The purpose of this policy is to provide Oak Park Police Department personnel with guidelines and principles for the use, collection, access, dissemination, retention and purging of ALPR data to ensure that the information is used for legitimate law enforcement purposes only and to ensure that the privacy, civil rights and civil liberties of individuals are not violated in connection with such ALPR data usage.

III. DEFINITIONS:

Automated License Plate Reader (ALPR): Any device that automatically scans the license plates of vehicles and using machine learning, interprets the alphanumeric values on the plate.

Automated License Plate Reader (ALPR) system: A system that includes ALPR hardware and software that processes license plates and other pertinent vehicle identifiers into a data system for searching and retrieval.

Law Enforcement Purposes: The investigation and detection of a crime or violation of law, excluding minor traffic enforcement. Examples include the searches for missing persons or vehicles involved in criminal activity.

Reasonable Suspicion: The standard of proof necessary for a police officer to engage in a temporary investigatory detention of an individual. Must be supported by specific and articulable facts for suspecting a person of criminal conduct.

IV. ADMINISTRATION OF ALPR DATA:

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access shall be managed by the Deputy Chief of Support Services. The Deputy Chief of Support Services will assign personnel under his/her command to administer the day-to-day operation of the ALPR equipment and data.

V. ALPR OPERATION:

Use of an ALPR is restricted to the purposes outlined below. ALPR devices and information contained within the ALPR database will be utilized for official and legitimate law enforcement purposes only. Department personnel shall not use, or allow others to use, the equipment or database records for any unauthorized purpose.

- A. No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.
- B. ALPR data shall only be used as an investigative tool for violent crimes, stolen vehicles and missing or endangered persons. The ALPR may be utilized for other significant felony offenses with a written request approved by the Chief of Police.
- C. An ALPR shall not be used to seek data on any individual or organization based solely on their religious, political, or social views or activities; their participation in a particular non-criminal organization or lawful event; or their race, ethnicity, citizenship, age, disability, gender, gender identity, sexual orientation or other classification protected by law.
- D. An ALPR shall not be used to target any group or individual in a discriminatory manner or infringe on constitutionally protected activities. This shall not preclude the Chief of Police or the system administrator from releasing general information as to the effectiveness of the ALPR equipment and other such communications.

- E. Use of the ALPR system for traffic enforcement and immigration enforcement is prohibited.
- F. All users of the ALPR system will abide by the Oak Park Village Code Reproductive Health Rights Article (13-8-1 through 13-8-6) and Illinois Reproductive Health Act (775 ILCS 55/1-35).
- G. Reasonable suspicion or probable cause is not required before using an ALPR. However, an officer may not detain an individual based on the alert from the ALPR system unless the officer has reasonable suspicion that such person is involved in criminal activity.
- H. Officers shall verify all ALPR activations prior to taking enforcement action. Verification should include the visual inspection of the scanned license plate image regarding the plate letters, numbers and issuing state. The officer should also verify the plate match of the vehicle in question by also comparing the vehicle's make and any other descriptors provided in the ALPR alert. Verification may also be assisted through the use of a query on the vehicle registration via the Illinois Law Enforcement Agencies Data System (LEADS).

Ground-based ALPR installation locations will be determined by the Crime Analysis Unit through multipoint crime analysis of current criminal incidents, historical criminal incidents and high-density violent crime areas. The recommendation of ALPR installation locations must be approved by the Chief of Police. Existing ALPR installations may only be relocated after receiving approval by the Chief of Police after following a similar analysis of criminal incidents near the proposed installation location.

VI. ALPR DATA COLLECTION AND RETENTION:

All data and images gathered by an ALPR are for the official use of the Oak Park Police Department and because such data may contain confidential LEADS information, it is not open to public review. ALPR information gathered and retained by this department may be used and shared with prosecutors or others only as permitted by law.

The database retention period for all data collected by ALPR hardware and stored on the ALPR cloud storage system shall not exceed 30 days. The ALPR system permanently deletes every 30 days on a rolling basis by default. The exceptions are if it is of evidential value in a criminal, civil action or is subject to a lawful action to produce records. In such circumstances, the applicable data should be downloaded from the server onto portable media and booked into evidence. Mass downloading of ALPR data via the ALPR cloud storage system is prohibited.

Collected ALPR data is encrypted and held in an AWS CJIS compliant cloud. Because this cloud is vendor owned, data contained in the ALPR cloud is not subject to request or disclosure under the Illinois Freedom of Information Act. Individual ALPR data records downloaded as part of an active investigation become records of the Department. Individual ALPR records that are downloaded for use in an investigation are subject to Illinois FOIA request similar to all other data and records belonging to the Department. Downloaded records are to be treated as evidence and stored according to Departmental procedures and policy by the ALPR end user. Evidence created through use of ALPR query shall also be included in an officer's/analyst's investigative report.

VII. ACCOUNTABILITY AND SAFEGUARDS

All saved data will be closely safeguarded and protected by both procedural and technological means. The Oak Park Police Department will observe the following safeguards regarding access to and use of stored data:

- A. All non-law enforcement requests for access to stored ALPR data shall be referred to the Records Division Supervisor and processed in accordance with applicable law.
- B. All ALPR data downloaded to the mobile workstation and server shall be accessible only through a login/password-protected system in accordance with the Village of Oak Park computer use policy.
- C. Persons approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.
- D. Such ALPR data may be released to other authorized and verified law enforcement officials and agencies at any time for legitimate law enforcement purposes. Electronic online sharing of Departmental historical ALPR data to external law enforcement agencies, who use a compatible ALPR system, is permissible and will be at the discretion of the Chief of Police. If the external agency request produces investigative leads in other jurisdictions, the Oak Park Police Department will not provide records from those external agencies to the requesting agency. The Oak Park Police Department will then refer the requesting agency to the outside agency where the original records reside.

When practical, and in absence of exigent circumstances, external law enforcement requests should be referred to the Investigations unit or the Records Department for processing and record keeping.

- E. Agency user audit reports will be produced and inspected monthly to ensure compliance with this policy. The system administrator will be responsible for conducting the monthly audit and reporting any discrepancies, problems or misuse to the Chief of Police. The monthly user audit will also contain anonymized user data and transactional data suitable for release on the Department's web-based Transparency Portal.
- F. The Chief of Police will provide the department's stops and any approved felony-related searches in a monthly report to Citizen's Police Oversight Committee (CPOC). In addition to the department's usage, CPOC will be supplied with the name and number of searches conducted by outside agencies.
- G. The monthly report will be an audit of activity for investigative value, policy adherence and disparate impact.
- H. Any Department member found to be in noncompliance with this policy in their use of the ALPR system will immediately have their access suspended to the ALPR system and be subject to the appropriate disciplinary actions. Any non-Departmental personnel found to have gained unauthorized access will be referred to the appropriate authorities for criminal prosecution, as necessary.
- I. If an outside agency is found to be using ALPR data for personal use, immigration enforcement and/or non-law enforcement purposes the department will revoke sharing access.

VIII. TRAINING

- A. The Department will establish end-user training for those employees provided direct access to ALPR data. ALPR system users shall be trained prior to being granted access to the ALPR system(s). Training will include:
 - 1. this policy
 - 2. Village of Oak Park Computer Use Policy
 - 3. proper handling/storage of ALPR downloaded records
 - 4. searching of the ALPR system(s)

5. requirements and process of creating and appropriate uses of ALPR technology
 6. possible penalties for ALPR policy violation.
- B. All ALPR users shall review and sign off on this policy every year.
- C. All ALPR users are required to obtain a LEADS certification every 2 years.

IX. ALPR DATA ACCESS PROCEDURES:

Access to the ALPR system for the purpose of queries will be granted to all Oak Park Police Department officers, dispatchers, and criminal analysts. Use of the ALPR system for queries must be related to an official investigation, personnel complaint, administrative investigation, or criminal investigation. All users that are granted access to the ALPR system will be issued a unique username and password specific to each individual user. The login will require multifactor authentication. The use of another employee's username and password is prohibited. The sharing of an employee's username and password is also prohibited. The use of the ALPR system outside of work devices is prohibited. Employees who separate from the Department or no longer need access to the ALPR system will promptly have access rights removed.

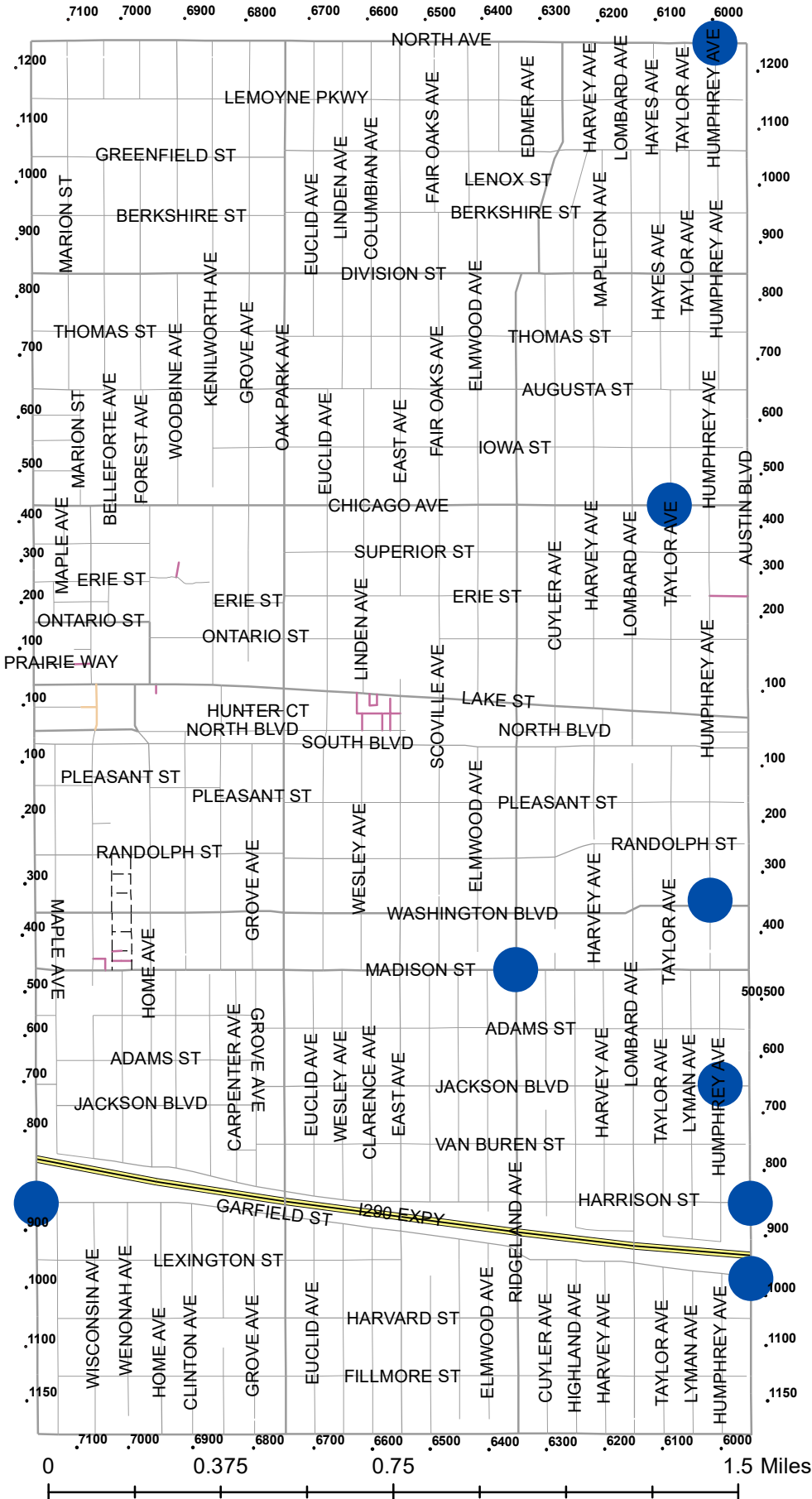
1. Police Officer user accounts will enable search capability across the Oak Park Police Department ALPR network and other agency ALPR networks from law enforcement agencies that have agreed to ALPR data sharing.
2. Detectives and criminal analyst user accounts will match those of Police Officers with the addition of creation and use of Oak Park Police Department Internal Hot Lists.

When conducting investigative queries into an ALPR database, the requestor is required to enter either a case number or a CAD run number with a short description as to why they are initiating the search. This entry will be associated with the search and be visible in the system audit logs. Queries regarding administrative or auditing purposes will be excluded from the requirement to provide a case number.


Shatonya Johnson
Interim Chief of Police

Blank Page

Village of Oak Park



FLOCK CAMERA LOCATIONS AS OF 20 JULY 2022

Blank Page

Four Common Issues from both Commissions and OPPD's Response

- (1) The use of the cameras for very specific crimes: stolen vehicles and violent crimes;
OPPD RESPONSE: General Order Section V. B. ALPR OPERATION was modified from "ALPR data shall only be used as an investigative tool for felony offenses and violent crimes."
~ to ~
"ALPR data shall only be used as an investigative tool for violent crimes, stolen vehicles and missing or endangered persons. The ALPR may be utilized for other significant felony offenses with a written request approved by the Chief of Police."

- (2) The ability to FOIA data in Flock Technology;
OPPD RESPONSE: This section of the General Order was not changed, because Flock confirmed that the FOIA only applies to data that is downloaded by the Police Department.

- (3) Granting access to only the partnering agencies that share our values;
OPPD RESPONSE: General Order Section VII. I. ACCOUNTABILITY AND SAFEGUARDS was modified from "If an outside agency is found to be using ALPR data inconsistent with our policy, the department will revoke sharing access."
~ to ~
"If an outside agency is found to be using ALPR data for personal use, immigration enforcement and/or non-law enforcement purposes the department will revoke sharing access."

- (4) CPOC should be able to monitor partnering agencies access to OPPD's camera.
OPPD RESPONSE: General Order Section VII. F. ACCOUNTABILITY AND SAFEGUARDS was modified from "As an added accountability, the Chief will provide the Citizen's Police Oversight Committee (CPOC) with a monthly report to review the types of stops"
~ to ~
"The Chief of Police will provide the department's stops and any approved felony-related searches in a monthly report to Citizen's Police Oversight Committee (CPOC). In addition to the department's usage, CPOC will be supplied with the name and number of searches conducted by outside agencies."

Blank Page

Thomas H. Ptacek

Oak Park Civic Information Systems Commission
thomas@sockpuppet.org

May 17, 2022

To: David Baker

Chair, Oak Park Civic Information Systems Commission

Chair Baker (and to whomever else this may concern),

Along with all the other members of the VOP CISC, I've been asked for feedback, recommendations, and action items regarding the proposed implementation plans for Flock ALPR cameras in the Village, including Flock's privacy policy and the privacy and data sharing implications of the OPPD General Order regarding ALPR cameras, communicated at our May 12th 2022 CISC meeting.

I'm on board with VOP's goal of implementing Flock cameras by the end of June 2022, but the plans presented to us at the May 12th CISC meeting fall short of the requirements set out by the board.

What follows in this letter is my feedback. At the conclusion of the letter, I've summarized my recommendations in a checklist.

The Flock Issue As Presented To CISC

CISC is reviewing the Flock implementation as a result of the amended motion to acquire Flock cameras put before the board at its meeting on April 4, 2022. I took the time to review and transcribe VOP President Scaman's statement regarding the cameras and CISC; a transcript is included at the end of this letter. I'd like to call out some specific language President Scaman used (emphasis mine):

I would be willing to vote "yes" on the original ask of 8 cameras, with the potential of increasing that number with the necessary data that justifies its need to our whole community, and holds us accountable as a government **utilizing it only when necessary, for strict stolen vehicle and violent crime alerts only** and never for traffic violation or other non-emergency stops.

[...]

My vote would be **fully contingent upon** a contract that can be canceled at any time (which we've heard tonight is the case) and **sending a protective policy to CISC that prevents misuse from our own personnel as well as other communities.**

Both CISC and CPOC are tasked with oversight of the implementation plan for Flock. It is my understanding that CPOC houses expertise on policing policy, oversight, and overall harm reduction from policing. Meanwhile, CISC's expertise is in technology, privacy, and transparency. With that in mind, I'll do my best to confine my feedback to areas of CISC's expertise, and leave to CPOC the broader questions of how OPPD should relate to people in the Village.

I believe the question put to CISC is simple: **does the implementation plan communicated to CISC at the May 12th CISC meeting conform to the Oak Park Village Board's authorization for Flock cameras, as amended at the April 4th Village Board meeting?**

My belief is that OPPD's planned implementation could, with small modifications, conform to that amended authorization, but that as currently stated it does not.

High Level Concerns With Flock Implementation As Presented

Concern 1: Purposes For Which ALPRs Can Be Used

The language of the OPPD General Order implementing Flock cameras currently reads as follows:

Law Enforcement Purposes: The investigation and detection of a crime or violation of law, excluding minor traffic enforcement. Examples include the searches for missing persons or vehicles involved in criminal activity.

Meanwhile, from VOP President Scaman's statement introducing the amended authorization on April 4th:

Requires — meaning I would like to forbid — forbidding access from other communities outside of those same uses of violent crime and stolen vehicles that we would use it for ourselves

At our May 12th CISC meeting, the example was presented of using Flock to track cars involved in the theft of catalytic converters from cars parked on VOP streets (a crime I've myself been a victim to). Representatives from OPPD confirmed in our recorded meeting that such thefts might meet the definition in the General Order of crimes to which Flock might be applied; for instance, OPPD noted, the drivers of cars involved in catalytic converter thefts might themselves be armed.

It's clear that the General Order as drafted does not match the intent of the Village Board in authorizing the use of ALPR cameras. OPPD has clarified that they'd intend to use the technology only to pursue felony cases. But felonies are not per se violent crimes. As drafted, and then confirmed by OPPD in our CISC meeting, OPPD sees itself as authorized to use Flock cameras to pursue property crimes in addition to violent crimes.

I have mixed opinions about the use of ALPR cameras to track package thefts, midnight garage lawnmower heists, and catalytic converter thefts. But my opinion

here doesn't matter: the board made it clear that there were just two cases in which VOP is comfortable currently using ALPRs: violent crime, and stolen vehicles.

If the Flock pilot rollout is successful, and the cameras help make stolen car, carjacking, and firearms cases, the board retains the option of broadening the use of Flock cameras in the future. But in the immediacy, the General Order needs to be amended; it should read something like:

Law Enforcement Purposes: Use of ALPR cameras are permitted only in the investigation of violent crimes, as defined by the FBI's Uniform Crime Reporting program, or stolen vehicles. ALPR cameras must not be used to investigate traffic violations, and must not be used for the investigation of property crimes or other non-violent crimes.

OPPD RESPONSE: This section was modified. Please refer to your 'Summary of Recommendations' #1.

Concern 2: Sharing With Other Law Enforcement Agencies

The Oak Park Police Department has a profound commitment to community engagement. That commitment is prized by village residents; indeed, words to that effect are invariably the first thing to come out of the mouth of any official discussing OPPD. I share that opinion. OPPD is fantastic.

My high opinion of OPPD emphatically does not extend to every other municipality in the Chicagoland area. Many communities in Chicagoland do not share Oak Park's values.

The terms under which Flock data will be shared with other communities are set out under Section VII of the enabling General Order, and read as follows:

D. Such ALPR data may be released to other authorized and verified law enforcement officials and agencies at any time for legitimate law enforcement purposes. Electronic online sharing of Departmental historical ALPR data to external law enforcement agencies, who use a compatible ALPR system, is permissible and will be at the discretion of the Chief of Police. If the external agency request produces investigative leads in other jurisdictions, the Oak Park Police Department will not provide records from those external agencies to the requesting agency. The Oak Park Police Department will then refer the requesting agency to the outside agency where the original records reside.

1. When practical, and in absence of exigent circumstances, external law enforcement requests should be referred to the Investigations unit or the Records Department for processing and record keeping.

Again, regardless of my own personal concerns about interdepartmental sharing of ALPR data, this language does not comply with the board's stated intent in authorizing Flock cameras (emphasis mine):

Requires — meaning I would like to forbid — **forbidding access from other communities outside of those same uses of violent crime and stolen vehicles that we would use it for ourselves.**

OPPD RESPONSE: Please refer to your 'Summary of Recommendations' #2.

More specifically, my observations about the language of the General Order are:

- A. No indication is given as to which specific law enforcement agencies will be granted access to Oak Park data. Will Berwyn have access? What about Chicago? What about Palos Park and Orland Park, which have publicly opposed Illinois policing reform measures?

OPPD RESPONSE: Please refer to your 'Summary of Recommendations' #2.

- B. No indication is given as to whether law enforcement agencies outside of Oak Park will be able to conduct retrospective searches on camera data collected in Oak Park, a core feature of the platform that enables police officers to create a “hit list” of license plates.

OPPD RESPONSE: Please refer to your 'Summary of Recommendations' #3.

- C. No indication is given as to whether law enforcement agencies outside of Oak Park will be able to add license plates to Oak Park’s Flock “hit list” of plates.

OPPD RESPONSE: Please refer to your 'Summary of Recommendations' #3.

- D. No indication is given as to whether law enforcement agencies outside of Oak Park can create “hit list” entries, or conduct retrospective searches, to investigate non-violent property crimes, or even traffic offenses.

OPPD RESPONSE: Please refer to your 'Summary of Recommendations' #3.

- E. Though OPPD emphatically states that our Flock deployment will not be used to facilitate US Immigrations and Customs Enforcement (ICE) investigations, the language of the General Order permits those uses.

OPPD RESPONSE: Please refer to your 'Summary of Recommendations' #4.

- F. No policy appears to exist under which access to specific municipalities might be rescinded if our Flock cameras are abused in their own searches; in

the current language, only OPPD employees are subject to discipline for misuse.

OPPD RESPONSE: Please refer to your 'Summary of Recommendations' #2.

- G. As explained at the May 12th CISC meeting, interactions with Flock are logged, along with a case number tying the interaction to a specific VOP-approved cause (presumably: a violent crime or stolen vehicle). This data is entered free-form, according to an OPPD standard. No language appears to exist requiring partner municipalities to conform to that standard, which would prevent CPOC from accurately tracking the uses to which partner municipalities put our cameras.

OPPD RESPONSE: Please refer to your 'Summary of Recommendations' #6.

Concern 3: Transparency and FOIA

A core premise of the Flock deployment in VOP is that VOP “owns the data” we generate, not Flock.

CISC hasn't been given a copy of the contract VOP has executed with Flock (along with any riders, terms, and statements of work that may be attached to that contract). So CISC cannot presently evaluate whether VOP “owns” Flock data even in theory.

Flock makes clear to VOP that data housed in Flock, in private server instances running in AWS GovCloud, are not subject to Illinois FOIA. It makes sense that Flock would maintain that: it cannot possibly be the case that Flock is fully subject to Illinois' ambitious FOIA statute simply by dint of signing a contract with VOP; no private company could operate under those terms.

But it cannot simultaneously be the case that VOP “owns” a tranche of data that is hidden from Illinois FOIA simply by dint of being stored in private AWS servers. VOP and OPPD are “Public Bodies” under 5 ILCS 140. We either own the data or we don't. If we own it, it constitutes a “Public Record”.

OPPD RESPONSE: This is addressed in Section VI. APLR DATA COLLECTION AND RETENTION, paragraph three:

Collected ALPR data is encrypted and held in an AWS CJIS compliant cloud. Because this cloud is vendor owned, data contained in the ALPR cloud is not subject to request or disclosure under the Illinois Freedom of Information Act. Individual ALPR data records downloaded as part of an active investigation become records of the Department. Individual ALPR records that are downloaded for use in an investigation are subject to Illinois FOIA request similar all other data and records belonging to the Department. Downloaded records are to be treated as evidence and stored according to Departmental

procedures and policy by the ALPR end user. Evidence created through use of ALPR query shall also be included in an officer's/analyst's investigative report.

I'll call out 3 specific concerns stemming from this conundrum:

- A. The shielding of data from Illinois FOIA for any reason other than the specific exceptions authorized by the Illinois General Assembly and Illinois courts is an indication that we do not, in fact, own that data. We should have a list of the data collected through Flock cameras (Flock will almost certainly already have this enumerated in their "Data Classification Policy", which is required by the SOC2 security standard they publicly comply with). With it, we should be able to itemize the data that we do and do not "own".
- B. OPPD clarified in our May 12 CISC meeting that data downloaded from Flock by OPPD (for case files and in reports) is subject to FOIA. OPPD must undertake procedures to maximize this data. No policies or procedures have been documented requiring OPPD to periodically export all available data, reports, logs, and configurations into records that can be obtained through public records requests. Policies need to be drafted that define:
 - a. The cadence at which reports from Flock will be generated and made available to records personnel.
 - b. The duration over which those records will be retained to respond to public records requests, complaint with VOP and Illinois public record retentions rules.
 - c. The data available from the Flock interface that can be exported to make available for public records requests.
 - d. Redactions and exclusions, compliant with Illinois FOIA, needed to protect privacy and public safety.

OPPD RESPONSE: Please refer to your 'Summary of Recommendations' #7.

- C. Whichever transparency steps VOP takes to ensure OPPD policy and records aren't hidden in a private database, those steps must also bind on partner municipalities. It's unclear based on the information given to CISC what records we'll even have of the searches conducted by other municipalities. For instance: will CPOC be given data about searches from partner municipalities in its monthly review of ALPR usage?

OPPD RESPONSE: Please refer to your 'Summary of Recommendations' #6.

Concern 4: Information Security

As communicated in our May 12 CISC meeting, OPPD intends to roll out Flock access to all OPPD patrol officers, as well as OPPD's one crime researcher (the sole person that will have Flock access who isn't a sworn officer).

OPPD employs approximately 100 sworn officers. OPPD personnel will access Flock over the public Internet, using Flock accounts with usernames and passwords.

As a professional with over 25 years of experience in information security, I can assert confidently that no organization with 100 members has ever kept that many passwords secure. Regardless of policies and procedures to protect passwords, they are invariably compromised: some member of OPPD will have an account with a related password on an unrelated service – a fantasy football league, an Internet message board, whatever – which will be compromised, handing attackers a giant database of passwords.

Flock Safety is a high-value target. Attackers will put in extra effort to hack accounts on it. The safety of Oak Park residents cannot be left to 100 usernames and passwords.

At our May 12 meeting, I asked a Flock representative whether Flock has features to require 2-factor authentication. Those features, common in SOC2-certified applications like Flock, *require* users to enable a second factor to log in. If such a feature exists, OPPD must enable it.

Flock may not have the feature that *requires* second factors for login to Flock. OPPD should add language to the General Order requiring officers to enable it explicitly.

OPPD RESPONSE: This was added. Please refer to your ‘Summary of Recommendations’ #9.

Additionally:

- A. OPPD should draft policy allowing access to Flock only from authorized OPPD computers; OPPD officers cannot safely access Flock from their home computers, which are not subject to OPPD’s Information Security policies and procedures.
- B. Flock must make available records of all accesses by OPPD staff (whether or not they involve a search or “hit list” addition), along with the IP addresses used for those access.
- C. OPPD should draft policy requiring a regular (quarterly or better) review of the IP addresses used to access Flock, so OPPD can enforce the rule forbidding access to Flock from insecure personal computers.
- D. Flock should make available documentation from its most recent security audits, including:
 - a. Any available SOC2 or SOC3 audit reports (these are provided as standard operating procedure in commercial product evaluations; the whole purpose of SOC2 is to make these reports available).
 - b. Evidence of recent third-party network security scans and penetration tests (again, standard operating procedure in commercial procurements).
 - c. Documentation about Flock Safety’s “Account Recovery” procedures, used to reset access to accounts whose passwords or

second factors have been lost; “Account Recovery” is a prime target for account takeover attacks.

OPPD RESPONSE: Please refer to your ‘Summary of Recommendations’ #11.

None of VOP’s safety and privacy goals matter if OPPD accounts on Flock are captured by attackers, who will laugh at the board’s amended authorization and OPPD’s enabling General Order as they mass-exfiltrate data directly from Flock. Even at companies with savvy security teams (Flock Safety is probably among them), “account takeover” (“ATO”) attacks are endemic.

Concern 5: Process

Finally, I want to raise concerns about the process and timeline under which CISC is providing recommendations to the board about Flock implementation.

VOP hopes to fully implement the Flock cameras by the end of June, 2022. The first formal engagement CISC had with VOP’s Flock plans was our May 12, 2022 meeting. Interim chief Shatonya Johnson emailed us a draft of the enabling OPPD General Order the day of the CISC meeting, on May 12th. It’s nobody’s fault that we’re on a breakneck timeline to get this done. But CISC has not been given adequate time to do any kind of formal review on the Flock plans.

OPPD RESPONSE: Although, CISC was given a week to review and provide feedback, all recommendations and feedback was accepted beyond the one-week timeframe.

In the ordinary course of CISC business, the process to generate feedback from the board would probably involve 3 CISC meetings:

1. A meeting like the one we had on May 12, to solicit information from VOP staff and Flock — that happened, and it was great, and I thank OPPD in particular for being generous with their time.
2. A followup meeting in which CISC would circulate a draft set of recommendations and opinions about Flock for discussion within the commission itself. There was no time whatsoever for that discussion on May 12th (which is a testament to how informative OPPD and Flock were!).
3. A final meeting in which all feedback from the first two meetings could be collected and distilled into a single document that the commission could vote on, for presentation to the Village Board.

OPPD RESPONSE: OPPD advised CISC that all emailed questions would be answered promptly. Additionally, CISC and CPOC would be provided in the final draft of the General Order with an explanation of what recommendations were not added.

That's not the process outlined by Village Manager Kevin Jackson. Instead, he related that he intended to collect whatever feedback we could generated based on the May 12th meeting, and whatever feedback he got from the upcoming May 25th meeting of CPOC, and then present it to the board.

It's understandable why VOP wouldn't want to run the "all-singing, all-dancing" full commission process for this. Due to the pandemic and limitations on when commission meetings can be scheduled, it's difficult to get CISC meetings together. Two additional full CISC meetings under our normal schedule would put us into July before we had formal feedback ready.

That said, we should come up with:

1. A clear set of deliverables for CISC and CPOC to provide to the board, so the board can approve the implementation plans for Flock and ensure it's being done according to the intent of the April 4 amended measure.
2. An expedited schedule for at least CISC (I don't want to make extra work for CPOC) to generate that deliverable.

It is not my understanding from hearing, transcribing, and re-reading President Scaman's amended authorizing measure that the intent of this process is to have CISC and CPOC make idle recommendations to VOP and OPPD; rather, I understand our role to be that of informing the Village Board, so the Village Board can exercise its actual authority over how Flock is rolled out, with out input.

Summary of Recommendations

1. The “Legitimate Law Enforcement Usage” definition in the enabling OPPD General Order should be narrowly scoped to “violent crime” (per a standard definition such as FBI’s UCR) and “vehicle theft”; in particular, mere “felonies”, which can include porch package thefts, should not at this point be grounds for ALPR searches.

OPPD RESPONSE: The definition will remain, because parameters for usage are specified in Section V. B. and E. ALPR Operation:

B. ALPR data shall only be used as an investigative tool for, violent crimes, stolen vehicles and missing or endangered persons. The ALPR may be utilized for significant felony offenses with a written request approved by the Chief of Police.

E. Use of the ALPR system for traffic enforcement, immigration enforcement is prohibited.

2. A list of the partner municipalities that will have access to VOP Flock data should be made available to the board.

OPPD RESPONSE: In an effort to maximize the effectiveness of the technology, OPPD will support in the reciprocal access sharing. If an agency has been identified as misusing the technology, OPPD will restrict their access.

As outlined in **Section VII. I. ACCOUNTABILITY AND SAFEGUARDS:**

If an outside agency is found to be using ALPR data for personal use, immigration enforcement and/or non-law enforcement purposes the department will revoke sharing access.

3. Partner municipalities and law enforcement organizations (LEOs) should be allowed to add license plates to VOP’s Flock “hit list” only in cases of “violent crimes” and “vehicle thefts”, and partner municipalities should not be able to conduct retrospective “make and model” searches of our cameras.

OPPD RESPONSE: Outside agencies cannot add to OPPD’s “Hot List.” Outside agencies are permitted to search the Flock technology, nationwide by license plate or make of a vehicle(s).

4. OPPD should track partner LEO usage of Flock cameras to ensure that all “hit list” additions are logged along with their cause, and that data should be made available to CPOC for their monthly review.

OPPD RESPONSE: Outside agencies cannot add to OPPD’s “Hot List.”

-
5. Explicit policy should be drafted to deny access to VOP's Flock data for purposes of immigration enforcement.

OPPD RESPONSE: There is a provision in the General Order that prohibits it in Section V. E. ALPR OPERATION: Use of the ALPR system for traffic enforcement, immigration enforcement is prohibited. In addition, OPPD will add this on the Transparency Portal.

6. Policy should be drafted to rescind access to specific partner LEOs for abuse of our Flock data, including searches or license plate "hit list" additions that do not include VOP-authorized causes (violent crime, auto theft).

OPPD RESPONSE: Our partnering agencies have their own policies that govern the effectiveness of their users.

7. Policy should be drafted requiring OPPD to periodically export and redact information from Flock, including searches made, accesses to VOP Flock data, configuration, and the list of partner LEOs granted access to our data, to ensure that the maximal amount of data is made available under Illinois FOIA.

OPPD RESPONSE: The OPPD does not have the resources to fulfill such a task. Flock maintains a log of all searches.

8. 2-factor authentication must be required for all users of VOP's Flock deployment; if an administrative setting is available in Flock to require it automatically, that setting should be enabled; the requirement to protect accounts with 2-factor authentication should be part of OPPD's written policy.

OPPD RESPONSE: This recommendation was added to Section VIX ALPR DATA ACCESS PROCEDURES.

Access to the ALPR system for the purpose of queries will be granted to all Oak Park Police Department officers, dispatchers, and criminal analysts. Use of the ALPR system for queries must be related to an official investigation, personnel complaint, administrative investigation, or criminal investigation. All users that are granted access to ALPR system will be issued a unique username and password specific to each individual user. The login will require multifactor authentication. The use of another employee's username and password is prohibited. The sharing of an employee's username and password is also prohibited. The use of the ALPR system outside of work devices is prohibited. Employees who separate from the

Department or no longer need access to the ALPR system will promptly have access rights removed.

9. OPPD should draft a policy allowing access to Flock only from authorized OPPD computers.

OPPD RESPONSE: This recommendation was added to **Section VIX ALPR DATA ACCESS PROCEDURES.**

Access to the ALPR system for the purpose of queries will be granted to all Oak Park Police Department officers, dispatchers, and criminal analysts. Use of the ALPR system for queries must be related to an official investigation, personnel complaint, administrative investigation, or criminal investigation. All users that are granted access to ALPR system will be issued a unique username and password specific to everyone. The login will require multifactor authentication. The use of another employee's username and password is prohibited. The sharing of an employee's username and password is also prohibited. The use of the ALPR system outside of work devices is prohibited. Employees who separate from the Department or no longer need access to the ALPR system will promptly have access rights removed.

10. OPPD should regularly audit access to Flock with IP-address logs of account access to ensure access is only occurring from authorized OPPD computers.

OPPD RESPONSE: **Officers are prohibited from accessing Flock technology on their personal devices as detailed in the response to Question 8 and 9.**

11. Flock should make available documentation from its most recent security audits.

OPPD RESPONSE: **OPPD required this information.**

12. An additional meeting of CISC should be conducted to circulate a draft set of recommendations the commission can vote on.

OPPD RESPONSE: **This is not an option. OPPD has provided a response to all of CISC's recommendations.**

-
13. The residents of Oak Park should buy interim chief Shatonya Johnson and newly hired Village Manager a pizza, or a cupcake, or something for putting up with persnickety CISC feedback.

OPPD RESPONSE: Nice gesture, but not necessary.

Sincerely,

Thomas H. Ptacek
Oak Park Civic Information Systems Commission
thomas@sockpuppet.org

Appendix: Village Boardm President Scaman’s Statement From Timestamp 2:32:15 At The April 4, 2022 Board Meeting Authorizing Flock

I am not comfortable with 20 cameras at this time. Plain and simply.

I would be willing to vote “yes” on the original ask of 8 cameras, with the potential of increasing that number with the necessary data that justifies its need to our whole community, and holds us accountable as a government utilizing it only when necessary, for strict stolen vehicle and violent crime alerts only and never for traffic violation or other non-emergency stops.

You know, as many stories as many Black persons in our community and many brown being stopped by the police, is the same for every single woman and every daughter and every mother, of unwanted sexual advances. It’s just a fact of life. And it’s going to unfortunately continue. But I do believe Oak Park can do better. And that is to the means of what I am suggesting.

My vote would be fully contingent upon a contract that can be cancelled at any time (which we’ve heard tonight is the case) and sending a protective policy to CISC that prevents misuse from our own personnel as well as other communities.

Requires — meaning I would like to forbid — forbidding access from other communities outside of those same uses of violent crime and stolen vehicles that we would use it for ourselves. I’d require the smallest window of time needed to solve crime before purging data, and that monthly reports of use are submitted to CPOC for review with the stated department policy shared with us as a board that responds to misuse with suspension from the platform and disciplinary action.

All these things have been outlined by our chief in a memo that we all received.

The reason for this decision is my belief that the use has solved crimes and that our department would otherwise continue with current access using other departments, other municipalities data, and we then lose any ability to track our own use and ability to hold ourselves accountable.

I fear that the only way we can address and even know if technology is being misused here or elsewhere is to own it. The technology will exist and will be used with or without our vote tonight. This way we will have the data we need to either yank it completely or not. And I, for one, will have no problem canceling the money spent on 8 cameras if it is not helpful or used without contributing to harm.

And, as we've heard, we'd also want to hear that data every 30 days.

I do believe that our police department is staffed by incredible human beings that care for our village. I have to check my own biases constantly and grateful for the people who help me do that. I do anticipate that, I know the police that we've heard this, we've heard the stories, we don't need to hear them again, that policing in general is human beings and biases exist and we need to do better.

I also need to see an ordinance that requires a board vote for the purchase of surveillance equipment of any kind above and beyond whatever we approve tonight forevermore.

This can never happen again.

Any changes in whatever our vote is tonight have to come back to the board table. Every single time.

I appreciate the expertise of our staff, but the world we live in now requires community engagement. We have trust to rebuild and mistakes like the process that led to today does nothing to help us rebuild trust in government. The need to hold ourselves accountable is not mistrust in staff necessarily or any person who works for the village of Oak Park. It is a mistrust in the systems that our criminal justice system and systems of oppression as a white person do not apply to me.

If I am wrong tonight, I will lean on our commissions to bring this back to us for corrective action. Hopefully corrective action that helps us be a better community overall.

So what we can do now is one of two things.

We can either vote on the agenda item that is presented, and it will presumably fail.

Or, if those who are interested in amending the motion, to read:

Approving a services agreement with Flock Incorporated for license plate recognition cameras and software for the purchase of 8 cameras and authorizing its execution contingent upon thorough vetting of a privacy policy by CISC and review of usage reports by CPOC on a monthly basis.

CISC Commissioner Wesley Flock System feedback, 5/17/22

Section III defines Law Enforcement Purposes as: Law Enforcement Purposes: The investigation and detection of a crime or violation of law, excluding minor traffic enforcement. Examples include the searches for missing persons or vehicles involved in criminal activity.

OPPD RESPONSE: The definition will remain, because the specifics when an officer can utilize the system are detailed in Section V. B. and E. ALPR Operation:

B. ALPR data shall only be used as an investigative tool for, violent crimes, stolen vehicles and missing or endangered persons. The ALPR may be utilized for other significant felony offenses with a written request approved by the Chief of Police.

E. Use of the ALPR system for traffic enforcement, immigration enforcement is prohibited.

However, my understanding is that this would be used only for major crimes. I think this language should be narrowed.

Section VII, E - " If an outside agency is found to be using ALPR data inconsistent with our policy, the department will revoke sharing access. "

We should not share data. The standards we hold our police to are higher than the standards other policing bodies are held to. By sharing access to our cameras with policing bodies who do not share our values, we are consenting to the use of FLOCK data in a way that is inconsistent with our values. A work around to this is a separate agreement with each law enforcement agency looking to access our data forcing them to agree to the same usage terms that we hold our local police to.

OPPD RESPONSE: In an effort to maximize the effectiveness of the technology, OPPD will support in the reciprocal access sharing. If an agency has been identified as misusing the technology, OPPD will restrict their access.

As outlined in Section VII. I. ACCOUNTABILITY AND SAFEGUARDS: If an outside agency is found to be using ALPR data for personal use, immigration enforcement and/or non-law enforcement purposes will revoke sharing access.

The database retention period for all data collected by ALPR hardware and stored on the ALPR cloud storage system shall not exceed 30 days.

I am uncomfortable with this length of time. The argument that there are too few cameras to create an effective timeline of a person's activities is compelling, but in the future there might not be only 8 cameras. Also, most major crimes will provoke near-instant investigations. As major crimes are the stated reasoning for using the FLOCK system, 30 days is an unnecessary risk to personal privacy. I think 7 days is more than reasonable, but would prefer 72 hours.

OPPD RESPONSE: This was not modified. Not all crimes are discovered and / or reported immediately. Additionally, evidential leads are identified at various times during an investigation.

Section IX - " When conducting investigative queries into an ALPR database, the requestor is required to enter either a case number or a CAD run number. This entry will be associated with the search and be visible in the system audit logs."

When providing the case number/CAD run number during the audit report, a synopsis of the case should be provided as well for review by the appropriate body.

OPPD RESPONSE: This was not modified. There is a section to provide a brief description. Flock advised that wordy descriptions make it difficult for administration to accurately audit searches. Additionally, the detectives will document any search results or lack of in a supplemental report.

Blank Page

Response to the Village of Oak Park and Oak Park Police Department

RE: Proposed General Order Regulating the Use of Automated License Plate Reader System(s) and Data

Presented to:

Village Manager Kevin Jackson
Interim Chief Shatonya Johnson
Trustee Chibuike Enyia
HR Director Kira Tchang

Presented by CPOC Members:

Kevin Barnhart kevbarnhart@gmail.com
Sue Humphreys sueehumphreys@gmail.com
Justin T. Johnson justintjohnson@gmail.com

June 1, 2022

Village Manager Jackson, Chief Johnson, Trustee Enyia, Director Tchang,

The Village of Oak Park (VOP) has engaged its Citizens Police Oversight Committee (CPOC) to review and comment on the Oak Park Police Department (OPPD) proposed General Order (Policy) for Automated License Plate Reader (ALPR) technology. At our CPOC meeting on May 25, 2022, committee members discussed the proposed Policy and were encouraged to submit questions, concerns, and suggestions to the VOP and OPPD.

This document, as well as a redlined version of the draft Policy, form the collective comments and recommendations of three (3) CPOC members (K. Barnhart, S. Humphreys, and J. Johnson) and do not represent the CPOC as a whole. Nevertheless, we look forward to your written reply regarding any questions or concerns that you may have based upon our suggestions, as well as welcome any additional dialogue necessary or desired to further clarify our comments, in the hopes of alleviating any such concerns. That being said, to the extent any of our suggestions are not accepted and integrated into the draft Policy, we would appreciate hearing your reasoning for any such rejection.

Thank you in advance for your time and consideration.

Brief Background/Basis for this Response

At its April 4, 2022 meeting, the VOP Board of Trustees voted to support the implementation of the Flock ALPR System to include eight (8) cameras and related software licensing, services, and support for OPPD to operate said system. This affirmative vote came with certain contingencies, as articulated by VOP President Vicki Scaman ([see recorded meeting here](#)). It is our opinion that these contingencies - *without which this vote would surely have failed* - boil down to the following agreements/understandings:

- The number of cameras is constrained to eight (8); additional cameras may not be implemented without clear and compelling data evidence to support their need
- The VOP may cancel its contract(s) with Flock at any time, without cause
- Implementation of ALPR technology must consider the needs of the entire VOP community and not target, inadvertently or otherwise, any particular area(s)/zone(s)/neighborhood(s), and/or demographic(s) of any type
- The OPPD must provide clear and compelling data evidence that implementation of ALPR technology does not cause nor contribute to harm nor violate the privacy, civil rights, or civil liberties of any individual
- Use of ALPR technology is prohibited for non-emergent stops, whether traffic-related or other
- Use of ALPR technology is restricted to stolen vehicles and vehicles suspected to have been utilized in the commission of a violent crime
- Any outside entity or person that accesses or uses VOP ALPR system(s) and/or data through any means or mechanism must agree to be bound by VOP ALPR General Order(s), policies, procedures, et al
- Implementation of ALPR technology is predicated on the Civic Information Systems Commission (CISC) review and approval of a privacy policy that governs how data will be collected, stored, accessed, interacted with/used, disseminated/shared, and retained - both internally and externally; such privacy policy must clearly identify how misuse of any kind will be prevented
- Implementation of ALPR technology is predicated on the CPOC review and approval of the OPPD Policy governing the use of the ALPR technology; such Policy drafted to ensure that the privacy, civil rights, and civil liberties of individuals are not violated by OPPD's intended use of the ALPR technology
- Monthly reports of use must be submitted to CPOC for review to ensure compliance with the final ALPR Policy, especially with regard to system misuse and potential disciplinary actions
- An Ordinance requiring a VOP Board vote, and governing the purchase and/or implementation of surveillance equipment of any kind, must be created and enacted prior to any future ALPR - or other surveillance technology - being implemented in or by the VOP

The remainder of this response addresses the contingencies and considerations listed above. We have attempted to organize these comments by topic and have repeated some of them in our redlined version of the proposed ALPR Policy for consistency and additional clarity.

System Use

1. To ensure compliance with the contingencies listed above, both the **CPOC and the CISC must be made aware of any/all updates to the Flock System sufficiently prior to proposed implementation in the VOP.** This includes receiving Flock user guides, data schema, and ongoing release notes for software updates, new modules, and/or new versions. It's our expectation that each Commission/Committee will focus its review of materials on their respective area of expertise, with the CISC primarily responsible for oversight of system/data privacy and transparency and the CPOC primarily responsible for oversight of system use especially as it pertains to community surveillance and the policing of marginalized populations. We will also pursue holding quarterly meetings between the CISC and the CPOC to discuss any updates or concerns re: the Flock implementation and ongoing system use and outcomes in general.
2. The proposed ALPR Policy must be **specific/consistent re: system use by internal and external actors.** The OPPD must identify everyone authorized to use the system, in what capacity, and to take which actions. **An audit log of all system activity should be maintained and shared with the CPOC** if we are to comply with the VOP Board request for oversight re: potential system misuse and resulting disciplinary actions. Moreover, the OPPD must provide updated rules/regulations and General Orders Handbooks that include potential violations and resulting disciplinary actions. With this information, the CPOC will be positioned to report on episodes of misuse to the VOP Board.

System use by outside individuals and/or agencies should be governed by a separate data sharing agreement between said parties and VOP or OPPD, as applicable, that requires adherence to the VOP ALPR Policy and use directives, at a minimum. Any misuse by an outside entity or individual must result in immediate revocation of all system access, at a minimum.

3. To address citizens' general privacy concerns pertaining to use of the Flock ALPR system, we encourage VOP/OPPD to **implement Flock's "opt out" or "safe list" capability.** This functionality appears to be a standard feature of the Flock system that allows vehicle license plates to be self-registered on a "safe list" which will automatically remove that plate from view/access/use in the system. As stated by the Flock representative on our 5/25 CPOC call, other governments/agencies are using this feature. Here's one such example:

<https://www.losaltoshills.ca.gov/FormCenter/Automatic-License-Plate-Readers-ALPR-Opt-22/Automatic-License-Plate-Readers-ALPR-Opt-154>

4. Our understanding is that OPPD has prohibited the use of Flock's "advanced search" capability that allows agencies to take a photo of a vehicle captured by another camera (e.g., cell phone or Ring doorbell) and upload it into Flock's system for search purposes. Should OPPD begin using this feature at any time, the CPOC and the CISC should be made aware as requested in 1. above.
5. Please explain how OPPD will use Flock in a scenario like this: a violent crime is reported at xxx Maple Street. Nearby cameras are searched for all vehicles in/out of that location. None of those plates trigger a "hit" for a vehicle meeting the crime definition contained in the ALPR General Order. Will system users be able to search for all vehicles in the area during the time of the crime? What will keep them from using that data to investigate the owners of those vehicles for whatever purpose they choose? How do we ensure that we are not - inadvertently or otherwise - causing potential harm in this scenario?

System/Data Transparency

1. When considering the needs of the entire VOP community, system/data transparency is clearly a top priority. To that end, we have noted several instances where the proposed ALPR Policy exempts ALPR data from public access/FOIA laws. It is our understanding that the VOP owns the data it collects and stores, regardless of where the data actually resides (i.e., whether in a Flock-supplied "cloud" environment, on-premise at OPPD, or in some other agreed-to location). As such, the data is considered public record and subject to applicable laws that govern public access. **If this is not the case, please include the specific statute(s) that exempt this data from public consumption/IL FOIA laws.**

While we are very interested in preserving (and enhancing) transparency and public accessibility of policing data, we are aware that CISC members bring significant industry expertise to this topic and we defer to their recommendations as discussed at the May 12, 2022 Flock meeting with CISC, and any subsequent recommendations from the CISC to the VOP/OPPD.

2. We understand that the OPPD intends to **implement the Flock Transparency Portal** and we encourage the use of this public-facing tool. We request that OPPD provide a list of all data that can be included for public viewing through this Portal and specifically identify the data that the OPPD intends to include in its implementation. At the least, we request that the OPPD include all the data in [this example from Piedmont CA](#).

Metrics and Measures

1. To support the contingencies that depend on evidence- or data-based decision making, the VOP/OPPD must include metrics and measures that will be used to determine success of the Flock implementation. How will the VOP gauge camera impact and/or effectiveness? What benchmarks are in place to help us ensure that the Flock implementation does not contribute to inequities in policing or compound harm? How will system misuse be determined? The OPPD has suggested that the Flock system will improve efficiency of investigations, and while that may be true, how will we prove this using “data evidence” as required by the contingent vote of April 4th?

We are making several recommendations that address this need for measures:

- a. The OPPD should snapshot incidents that meet ALPR Policy (final version) crime definitions for monthly and year-to-date comparisons that include: number of incidents by zone, incident offense(s), length of incident investigation, incident outcomes... and any other criteria that help to illuminate Flock System value when compared to pre-Flock crime statistics.
- b. If the OPPD is going to place cameras in response to crime “heat maps” as discussed at multiple meetings, it is important to then gauge individual camera effectiveness based on the impact of each camera to its corresponding zone within the “heat map”. We recommend that the OPPD specify this criteria including: what determines camera placement (how many of what crimes in what time period) and the threshold for removing or relocating a camera (e.g., 90 days of not meeting camera placement criteria). This camera placement and removal criteria should be public information, and subject to the CPOC approval. Additionally, continued use of a camera that does not meet placement criteria should require VOP Board approval.
- c. To demonstrate adherence to ALPR system use policies, the OPPD should produce one or more monthly reports to be reviewed by the CPOC. These reports should include at a minimum:

General Use: including number of vehicle detections (by camera), number and type of logins (including date/time, user, user title, user agency/department, action(s) taken), number and type of searches (including date/time, user, user title, action(s) taken) NOTE that “actions taken” assumes all activity pertaining to one or more records on the system – e.g., added, edited, downloaded, hot listed, shared, etc.

ALPR Records Downloaded including % of total records; date/time, user, user title, user agency/department, records downloaded, downloaded reason,

action(s) taken.

ALPR Records Resulting in Vehicle Stops or Individual Detainment (see the report example provided by the OPPD to the CPOC) in addition to what was proposed (stop number, vehicle plate, stop location, stop reason, stop result, demographics of persons stopped), please include: % of total records, officer ID, and officer demographics. Please also add a “gender” option for people identifying as non-binary. If a stop results in a search of a vehicle or its occupants, please include the results of that search (i.e., what was found).

- d. We’ve noted that in the proposed ALPR General Order, Section V, Item D, states that the Chief of Police or the system administrator may “... release general information as to the effectiveness of the ALPR equipment and other such communications”. We’d like to understand what general information this may include and what criteria the OPPD will use to determine “effectiveness of the ALPR equipment”. Once we better understand what is meant by this paragraph, we may suggest that the same information/data be included in one or more of the reports identified above.

Conclusion and Next Steps

We recognize that this response along with our redlined version of the proposed ALPR Policy will be reviewed and considered along with other responses from CPOC and CISC members. We have attempted to be as complete and concise as possible considering the directive given by VOP President Vicki Scaman at the April 4th Board meeting and the time constraints in providing this followup from our May 25th CPOC meeting.

Following your review of all responses, we anticipate that another conversation will be scheduled to answer questions and/or review an updated draft ALPR Policy. Ideally, the VOP/OPPD will hold this conversation with both the CPOC and the CISC together, allowing us to more clearly delineate roles and responsibilities for ongoing oversight of the Flock ALPR implementation and use. As per our understanding of the directive from President Scaman and the VOP Board, deployment of the Flock system should not proceed until such conversations have occurred.

Respectfully,

CPOC Members:

Kevin Barnhart

Sue Humphreys

Justin T. Johnson

Blank Page

CPOC QUESTIONS

Committee Member Jack Powers:

During last night's CPOC meeting, I asked this multi part question and feel I was given a solid, reasonable answer but wanted to reconfirm my understanding.

- 1) Flock system will alert OPPD in real time (30-40 second lag) of any plate that the cameras capture that is for a car that has been stolen, involved in a carjacking, is registered to someone suspected of a violent crime such as assault & battery, armed robbery, weapons charges, murder, manslaughter *and other felonies*. Basically, the system is hard coded to send alerts for these types of issues *only*.

Flock Safety will only generate alerts for stolen vehicles, wanted vehicles, stolen license plates and missing persons. The department has the capability to deactivate any of the aforementioned fields. In addition, the department can create a hit list for vehicles we seek to locate for violent offenses/felony offense.

- 2) Flock system sends no alerts for plates captured other than the above crimes, the data exists for 30 days and is permanently purged *unless* an officer investigating a reported crime after the fact accesses the Flock system within 30 days in the normal course of the investigation to see if helpful data is available. In other words, if no officer accesses Flock data for a particular plate or timeframe, the data is purged unreviewed by OPPD.

Correct, all the data captured by Flock cameras will be permanently purged, unless a detective download as evidence related to an investigation.

- 3) If 1 & 2 above are accurate, then would the Flock database be used no differently than databases currently used by OPPD in investigating reported crimes? For example, if an officer pulled over a car for running a red light (not because of a Flock alert), the stop would include a routine check of the license and registration, and if those checks revealed other pending issues for the officer to address, then the other issues would become part of that traffic stop? Or, for example, theft of packages from a porch might include a doorbell video showing a vehicle that might be crossed checked against the Flock system? Likewise, a catalytic converter theft where a doorbell or other security camera records the theft and a suspected vehicle?

This is correct, Flock Safety would be utilized as any other investigative tool.

One question I didn't ask is how can we be assured that a motion sensing camera won't capture images from the front of the vehicle thereby recording the driver's and front seat passengers faces? I can imagine how on narrow residential side streets like those in southwest Oak Park cars have to cross at least partially onto the other side of the street to get around parked cars, thus triggering the camera meant to capture images of cars going the opposite direction.

Flock cameras can capture as many as four lanes of traffic and may inadvertently capture the front plate of a vehicle and images of the occupants. I am not sure if there's anything that can be done to prevent it. However, people images are not searchable through the Flock technology.

Committee Member Dana Wright:

- 1) The first sentence of this section describes LE purposes for using ALPR as being detection of a crime or violation of the law. However, the examples in the next sentence include "searches for missing persons". Searches for missing and/or endangered persons is not always criminal, but can be helpful uses of the system. Can the purpose be written to include "non-criminal searches", i.e. people experiencing a mental health crisis, dementia, etc..?

Flock cameras will be utilized to search for vehicles in connection with missing persons. Flock technology does not have the capability to search for images of people. This section will be modified to alleviate any confusion. (Subsection III)

- 2) Again, this only addresses felony offenses or violent crime. Will uses for non-violent or non-criminal be acceptable if it is for missing or endangered persons as described in the first comment above?

The Flock cameras will be used as an investigative tool in violent criminal offenses and other felony offenses as well as missing person investigations. This section will be modified to alleviate any confusion. (Subsection V.(B))

- 3) Would permissible searches include non-violent/non-criminal offenses such as missing or endangered person (mental health crisis, runaway, dementia, etc.) that may have been entered into a hotlist?

Permissible searches added to the department's hotlist would include violent criminal offenses, other felony offenses and vehicles related to missing person investigations.

- 4) With the ALPR system only collecting license plate information, how would CPOC know of disparate impact? Will the report include additional stop data with each associated alert?

All alerts resulted in a stop will be provided to CPOC on a monthly report. A draft copy of the monthly report which includes the data that will be collected was sent in advance of the meeting. The Flock Safety system is objective, the license plates images are for investigative purposes this takes the human bias out of the equation.

- 5) For purposes of consistency when reviewing reports in the future, what code of conduct violation will be attached to violating the use of another employee's username/password or sharing of a username/password?

The violations could vary depending on the circumstances. The most common violation would be

- Rule 6: Obedience to Laws, Rules and Regulations, Policies, Procedures and Directives.
- Specifically, the ALPR General Order and the Village Technology Policy.