Project Alastor
An Evaluation of the Flock Camera System
In
The Village
Of
Pentwater

Submitted

October 12th, 2026

by

Chief Laude Hartrum

Table of Contents

Project Alastor Implementation History 3
Automated License Plate Reader Technology 4
Flock Group, Inc. 4
Automated License Plate Reader Technology in Pentwater 5
Camera Placement 5
Software & Access 6
DATA Sharing and Retention 6
FINDINGS 8
Camera Location 8
Desktop Software 9
How the system was used 9
Financial Impact 10
Civilian Oversite 10
Success Stories 10
Public Input 11
Civilian Evaluation Team 11
ANALYSIS AND RECOMMENDATIONS 12
Conclusion 13
Flock Safety Agreement 15
Submitted Public Comments 16
Shared DATA File 17

Project Alastor
Implementation History

In 2025 the Village of Pentwater became aware of an opportunity to conduct a demonstration project with Flock Safety. The project, later named Project Alastor resulted in the deployment of 10 automated license plate reader cameras at designated locations through the Village.

In May of 2025 the Police Department entered into an agreement with Flock Safety to deploy 10 cameras for a period of 90-days, after which the Village of Pentwater would have 45 days to decide whether to keep all the cameras, some of the cameras or remove the cameras. There was no cost for the cameras or services.

During the spring of 2025 Chief Hartrum worked with Flock Safety to determine the locations of the cameras and between May and June of 2025 work began to deploy the cameras.

Four areas of the Village were selected for camera placement; first, near the Pentwater Public School; second, near Channel Lane Park and Charles Mears Park; third, near the Pentwater Department of Public Works; and fourth near Chester Street and Ridge Road. One camera was deployed at the corner of Sixth Street and Hancock Street.

These cameras were to be located so that they would work in association with other Flock Cameras which had been scheduled to be installed via a separate agreement called Project Prove It. Project Prove It was the responsibility of the Oceana County Sheriff's Office.

All the cameras that were identified to be installed under Project Alastor were not installed. Only six of the cameras were installed. This was due to the fact that permits required to install cameras outside of the Village of Pentwater were not obtained.

When it became clear that cameras that were to be installed under Project Prove It were not going to be installed in time to meet the requirements previous agreed to, Chief Hartrum contacted Flock Safety and was told that all the cameras installed under contract

with Pentwater Police i.e. Project Alastor would remain in place until the summer of 2026 when, Flock believed Project Prove It would be ready to proceed. At that time the official 90-day demonstration project would commence.

On July 31, of 2026 Chief Hartrum received notice that the 90-day demonstration project had officially started. The 90-day demonstration project will end on October 30th of this year.

Automated License Plate Reader Technology

Automated license plate reader (ALPR) technology—called automatic number-plate recognition (ANPR) in the United Kingdom—grew from advances in video imaging and optical character recognition. The British Police Scientific Development Branch developed early systems in the 1970s, with working prototypes by 1979. Tests were conducted on major roads and at the Dartford Tunnel, and a plate-reader alert reportedly helped police identify a stolen vehicle in 1981.

During the 1990s, faster computers, improved cameras, infrared illumination, and less expensive recognition software made technology more practical. British authorities expanded its use in road networks and centralized plate data, while U.S. agencies began adopting similar systems in the late 1990s and early 2000, initially at border crossings and later on patrol vehicles. These mobile systems could scan plates rapidly and compare them with lists of stolen, wanted, or otherwise associated vehicles.

By the 2010s and 2020s, ALPRs had evolved into networked systems using fixed roadside cameras, vehicle-mounted units, and cloud-based databases. Modern systems record a plate image and number together with the time and location, then can issue near-real-time alerts or support later investigations. (https://en.wikipedia.org/wiki/Automatic_number-plate_recognition)

Flock Group, Inc.

Flock Safety is a private public-safety technology company that provides automated license plate reader cameras and related cloud-based software to law enforcement agencies, businesses, schools, and communities. Its cameras capture license plates, vehicle characteristics, and the time and location of a vehicle sighting, allowing authorized users to search for investigative leads or receive alerts when a vehicle matches an approved hot list. The system is intended to identify vehicles rather than people and does

not use facial recognition. (https://www.flocksafety.com/products/license-plate-readers#:~:text=Nation%27s%20largest,recognition.)

Automated License Plate Reader Technology in Pentwater

In 2011 under a grant, Pentwater Police installed one 3M PIP Automated License Plate Readers onto one patrol vehicle.

The ALPR compared license plates to state and federal databases in an attempt to identify vehicles associated with active warrants, known criminal and terrorist or suspected terrorists. Pentwater Police maintained the system for several years but ultimately could not afford to replace the system. The system was removed from the car 2013-2014.

Camera Placement

Chief Hartrum worked with Flock Safety to determine the best location for the cameras. Flock agreed to put in as many cameras as possible. Chief Hartrum and Flock decided to put in 10 cameras.

Camera locations were based on expected traffic flow. The assumption being that these locations would have the highest number of vehicles.

Camera #	Location	Direction
1	3rd Ave at E Hanover	SB
2	E Park St at W Hammet Rd	WB
3	W Lowell St at N Medford St	WB
4	N Mears St at Channel Lane	WB
5	S Hancock at Sixth St	NB
6	E Park at 3rd Ave	NB
Not Installed	North Madison @ DPW	EB
Not Installed	North Madison @ DPW	WB
Not Installed	Longbridge @ Ridge Rd	WB
Not Installed	Chester St @ Longbridge	SB

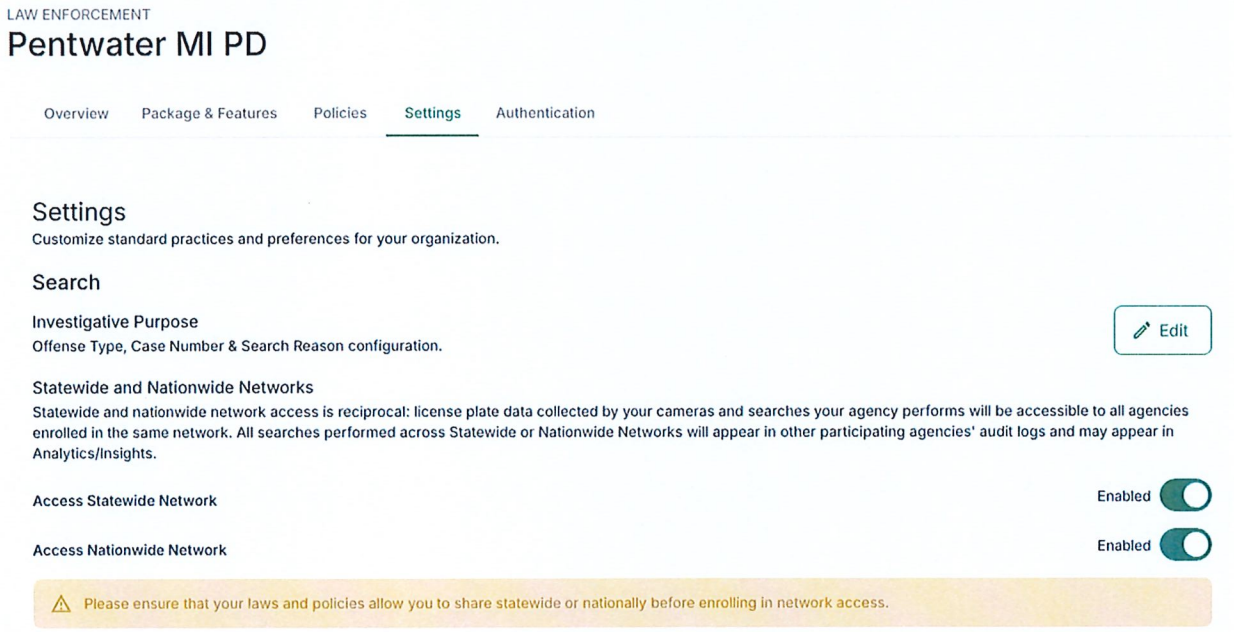
Software & Access

As part of Project Alastor, two methods of access were provided; a web-based portal and a app available for cell phones. Both methods were used by officers during this demonstration project.

DATA Sharing and Retention

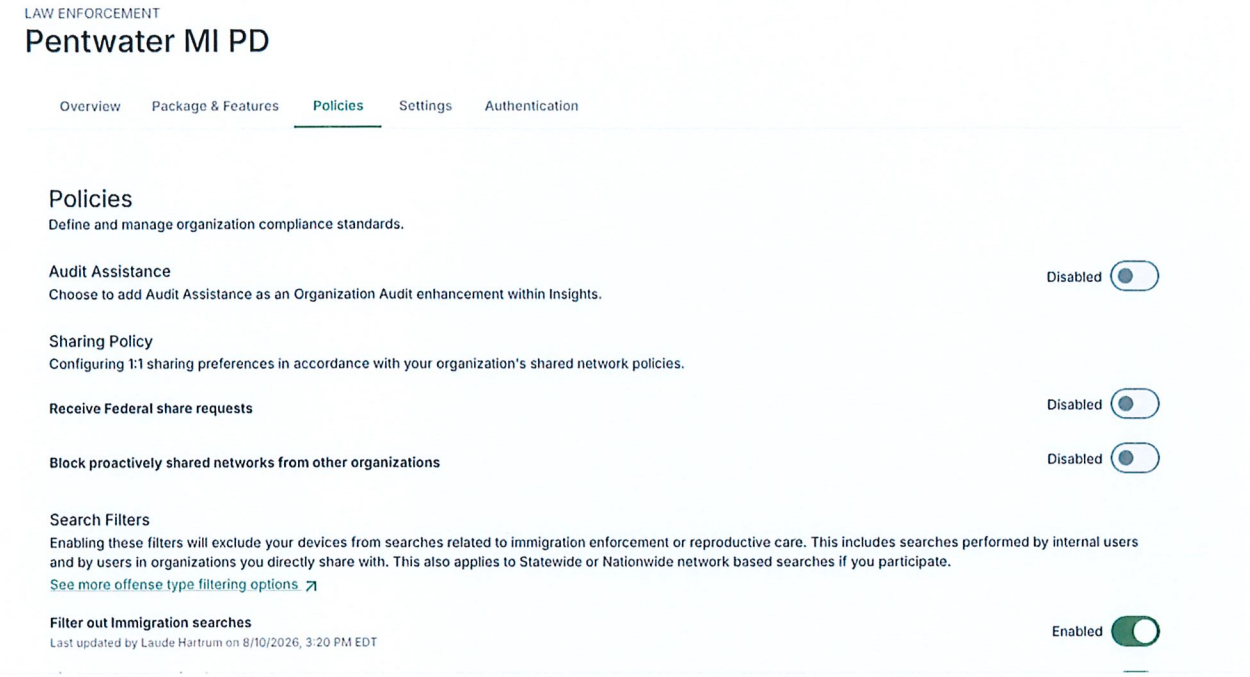
At the onset of this Project data was shared statewide and nationally. Beginning in July, data was restricted to Michigan agencies only. Currently we are sharing with approximately 262 agencies statewide (SharedNetworks_2026_September_22.CSV).

The Flock System offers several methods to restrict access to data.



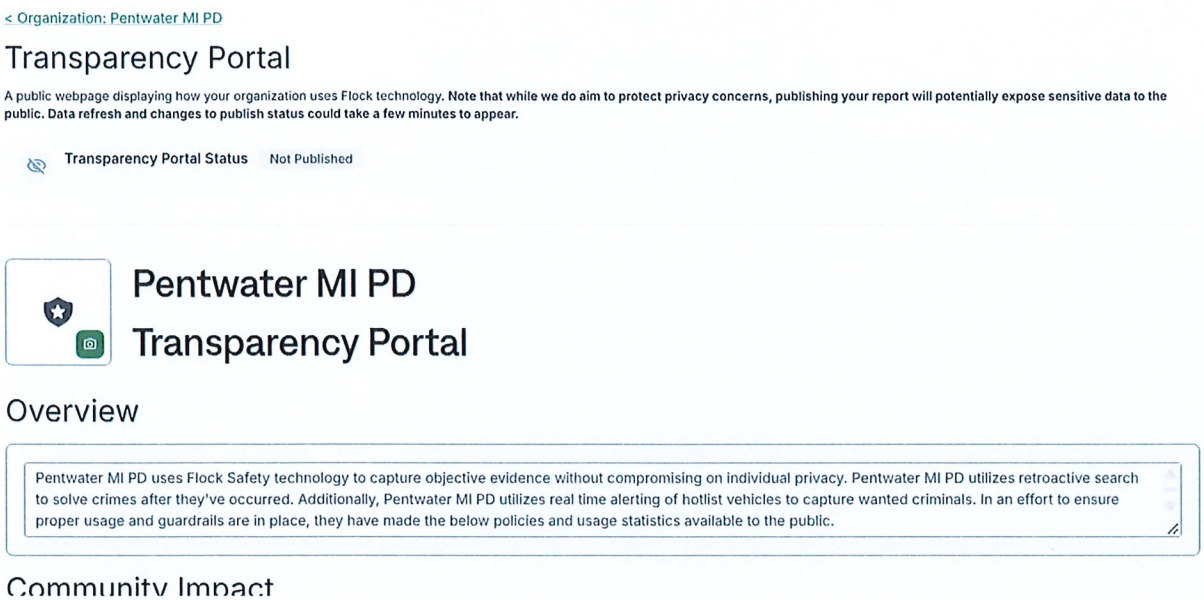
In the setting tab of in administration section of the software administrator can set required fields; Offense Type, Case Number and Search Reason.

Administrators can also enable access to statewide networks. Note that administrators have enabled the option to allow access to nationwide networks,



Under the Policy tab administrator can enable / disable access to audit assistance, sharing policy. Note that during this demonstration period the "Filter out immigration searches" was enabled.

Flock does offer a "Transparency Portal" which once enabled allows the public to search view the following reports; Cases Resolved, Success Stories, Camera Alert Activity, Data Retention, Camera Counts, LPR Cameras, Unique Vehicle Detected, Number of Searches, Hotlist Alerted On, Number of Hotlist Hits, Top Offense Types, List of Networks PPD are sharing with, List of Networks PPD is receiving data from, What is detected, What is not detected, Acceptable Use Policy, Access.



This option has only recently been available and was not used during this demonstration project.

All data collected by Flock Cameras is owned by Pentwater Police Department and stored via Amazon Cloud Storage. There are now two options for the length of time data is stored, 7 or 30 days. After the designated length of time the data is no longer available. The length of time is determined by Pentwater Police Department.

During this project the length of time was set to 30 days.

FINDINGS

Camera Location

While original plans called for 10 cameras to be installed, in fact only 6 cameras were installed.

The original camera locations were identified using the following criteria; first, where the cameras would see the most vehicles; second, cameras should be set to enhance security to critical structures; third, how they would enhance the County wide system.

Cameras that were in residential areas; Park Street and 3rd Ave, Channel Lane and Mears St. resulted in questions from area residents. These residents and property owners were concerned that the cameras were live and recording their movements.

In fact, this was not happening. The cameras only take photographs of vehicles and license plates. All that said, residents and property owners were still concerned.

It is recommended that cameras should be placed in area where residential homes are not present. Cameras should be placed so that views of homes and driveways area are limited.

A cluster of three cameras were located in and around Pentwater Schools and the Artisan Center. While these cameras did allow for increased security around the school. It is not practical to have three cameras in such a small area. It is recommended that Flock Cameras not be used near the Pentwater School.

A cluster of two cameras were located on the west side of Pentwater, specifically; Lowell Street at Charles Mears State Park, and Channel Lane at Mears Street. Again, It is recommended that Flock Cameras not be clustered in such a small area.

One camera was located at Sixth Street and South Hancock Street. This camera was not in a residential area and allowed the Department the ability to search for northbound traffic on Hancock Street.

The original plan included cameras located at the north, south, and east of the Village. The north and south cameras were to be located outside of the Village at North Hancock Street near the entrance to the Cemetery and another on Longbridge Road and Monroe. These two cameras were to work in association with a camera located on East Park Street east of 3rd Street. The only camera installed was the camera at East Park Street and 3rd Street.

Desktop Software

The desktop software used to access Flock Cameras was easy to navigate and operate. It allows administration of the system and searches of the cameras. It also provided the ability to develop localized "Hotlists" for investigative purposes.

The mobile app also was easy to navigate. The mobile app is the preferred method of getting alerts. However, it does require that the user has the app open and that notifications are enabled.

There were no issues with either the desktop software or the mobile app.

How the system was used

The system was used in the following ways.

1. A "Hotlist" was used to alert to suspected narcotics traffickers, vehicles involved with custody disputes (Pentwater School) as an early alert system.
2. The system was used to search for suspect vehicles. Once investigators had obtained a description of the suspect vehicle; make, model, year, color. Searches

were performed in an attempt to get a license plate of vehicle matching the description.

Financial Impact

Each camera represents an annual expense of $3000.00 plus $6000 for software and service. This is an annual cost of $ 36,000 for 10 cameras. In this case 6 cameras would cost $24,000 per year.

As the Police Department does not have $24,000 in their existing budget this money would have to be allocated from the general fund.

Civilian Oversite

During this Project there was no civilian oversight of the operations of this system.

Success Stories

Case # 26-65600023 Stolen Trailer

Flock Cameras were used in this case after receiving a description of a suspect truck used to steal the trailer. Specifically, the Flock Cameras provided us with a license plate and picture of the suspect vehicle. The vehicle was tracked down in Pierson Michigan through additional investigation and recovered. The suspect in this case gave investigators a full confession and has since been sentenced. Approximately $22,000 worth of stolen property was received.

Case # 26-65600131 Death Investigation

Grand Haven Department of Public Safety used a Flock Camera search to focus a search for a missing person out of their jurisdiction. The information was relayed to Oceana County Sheriff's Office who upon hearing that Pentwater Police had been sent to a submerged vehicle, contacted Pentwater Officers.

In this case the images were used to focus the search to Oceana County. The case remains active and no further details can be released at this time.

Public Input

In June of 2025, PPD received a cease-and-desist letter from a Pentwater Resident. The resident cited violations of their fourth amendment rights to the placement of the cameras and demanded that they be taken down.

In July of 2025, PPD was contacted by a resident. The resident was concerned that their home was under surveillance 24/7 by a Flock Camera on Park Street. PPD responded to the letter and provided images taken from the camera which showed the field of view. The resident was told that we were conducting a demonstration project and the status of that project at that time.

In July of 2026, PPD received a letter from a Bass Lake resident requesting that the cameras be removed because they represented an unwarranted surveillance of citizens. The resident went further saying that the technology was unreliable.

In July of 2026, PPD received an email from a Pentwater resident. The resident questioned why, if the Sheriff's Office had terminated their Project, PPD was continuing its Project. PPD repied and told the resident that an evaluation report would be submitted to the Village Council and that the Project would end in October, at which time the council would make a final decision.

In July of 2026, PPD received a letter from a long-time resident of Pentwater expressing their concern over, the purpose, and the necessity to have cameras deployed in Pentwater. The resident cited court cases, a concern about mass surveillance, and the use of the cameras in reproductive rights and immigration investigation. PPD responded and advised the status of the Project.

Over the last six months PPD has had two residents come to the Department and actually review the desktop software. They were shown how the searches were made, and who data was being shared with. After seeing the software in use, both expressed that they could see how the software would be useful to law enforcement. However, both were concerned that "AI" unmonitored would use the data for unintended purposes.

Civilian Evaluation Team

On Setember17th, 2026, PPD met with three residents of Pentwater who agreed to assist in the evaluation of the Flock Software. They reviewed the contract with Flock Safety, the software, and were briefed on the successful investigation that had conducted using the Flock System.

In sum, all the members of the team agreed that the technology could on its face be useful to law enforcement. However, they raised several concerns.

There was a concern about the ownership and retention of data collected using the cameras. While all understood that Pentwater Police owned the data, there continued to be a concern that Flock would use the data for other purposes not approved by the Department.

Team members were further concerned that the initial contract with Flock did not include the terms and conditions of the agreement.

There was a concern about the security of the actual camera. Even though each cameras memory card is encrypted, there remained a concern that hackers could crack the encryption at the camera location and gain access to the data.

Another issue raised was the penalty for unauthorized use of the data. The team cited reports of instances of police officers using the system to track ex-wifes / husbands or conduct surveillance of past boyfriends or girlfriends. There are no laws strictly governing unauthorized use of the data. In instances of misuse, penalties would be administrative and would not result in a criminal charge.

The team expressed concern over the implied sense of surveillance the cameras posed in residential areas.

The team further observed that while the cameras themselves were straightforward in there abilities, the software behind the cameras was constantly evolving and that the given the right software the camera's ability to do other things might at some point include facial recognition.

The team recognized that public distrust of Flock Safety was very high. The team cited numerous news articles, social media posts, observed that Flock Cameras had now become a political issue talked about by current candidates for elected office.

One team member commented that officially implementing the cameras might be the right decision but the amount of public outcry might not make it worth it, i.e. the benefits of the cameras might not be worth the political / financial cost.

ANALYSIS AND RECOMMENDATIONS

ALPR technology had been in existence for over 50 years and is commonly used in other states. Examples include tollways and red-light enforcement. The technology is not in

question. What has changed is the ability to conduct analyses and organize the data and the implications of this ability on the right of US citizens.

The purpose of Project Alastor was to assess the value of ALPR technology offered by Flock Safety and to learn if and how this product could be used to assist the Police Department. Additionally, Project Alastor was designed as a way to communicate with the citizens of Pentwater, educating as well as listening to issues that arise. Project Alastor was successful and achieved these goals.

It is our recommendation that the Village of Pentwater does not contract Flock Safety for the use of their systems. This recommendation is based on several issues.

First, the cost of Flock cameras is extremely high $3,000. The cost of six cameras is approximately $24,000 annually. The financial impact on the Police Department budget is significant.

Second, prior to the implementation of any ALPR technology it is strongly recommend that a citizen oversight committee or group be put in place to monitor the use of the technology in Pentwater. This group would help evaluate future camera systems and provide transparency for the residents of the Village of Pentwater.

Third, that the Pentwater Police Department continue to investigate alternative ALPR systems with an emphasis on system that includes; local data storage, and secure operating platform and minimal exposure to the public.

Conclusion

While many of the public concerns and comments focused on the control of data, unauthorized access to the data, and potential misuse of the technology, several residents questioned the need for ALPR technology in a Village the size of Pentwater.

There is a need for this type of technology in the Village of Pentwater. Perpetrators of crimes will focus on areas when they are unprotected, either by technology or by physical security. This has been observed and validated many times.

If the Village of Pentwater and the Police Department do not adapt and use new technology to help prevent crime, unscrupulous individuals who wish to perpetuate crimes will use the technology against us to their advantage.

The Pentwater Police Department partners and collaborates with all Oceana County and Mason County Law Enforcement agencies as well the Michigan State Police. These partnerships are vital to our ability to apprehend those who perpetrate crimes.

Currently residents are under surveillance from local Ring cameras, the Village Green Cameras, the Pentwater Yacht Club Cameras, and numerous other private cameras and trails cameras. Residents do not own or control this data.

ALPR, Facial Recognition, DNA analysis, Fingerprint Analysis, Polygraph Units, Drone Technology, Underwater Autonomous Drones, and Link Analysis along with other new technologies will and are being used in the State of Michigan.

Artificial Intelligence is used in cell phones, iPads, and other commonly used devices. Today, the debate about AI and its uses is ongoing, where and what the results of that debate will be are yet to be determined.

What is of vital importance is that communities and their police departments work together to decide how to best use these technologies to keep their communities safe.

It is our sincere hope that Project Alastor can act as a model for how the Pentwater Police Department will evaluate new technology as it moves forward in the 21st century.

The Department wants to thank all the citizens who contributed to this report. Hopefully we've conveyed everyone's concerns, questions, and comments.

Flock Safety Agreement

Docusign Envelope ID: D81128EE-7794-47ED-8B68-B883057EBADE

Flock Safety + MI - Pentwater PD

Flock Group Inc.
1170 Howell Mill Rd, Suite 210
Atlanta, GA 30318

MAIN CONTACT:
Agustin Campuzano
agustin.campuzano@flocksafety.com
+12142413822

flock safety

Docusign Envelope ID: D81128EE-7794-47ED-8B68-B883057EBADE

flock safety

EXHIBIT A
ORDER FORM

Customer:	MI - Pentwater PD	Initial Term:	12 Months
Legal Entity Name:	MI - Pentwater PD	Renewal Term:	12 Months
Accounts Payable Email:		Payment Terms:	Net 45
Address:	Po Box 622 Pentwater, Michigan 49449	Billing Frequency:	Annual Plan - Invoiced at the end of the pilot period.
		Retention Period:	30 Days

PROJECT PROVE IT

Customer will have a 90 day opt-out period ("Opt-Out Period") after implementation of the first Flock Hardware to terminate this Agreement without penalty or fees. After the Opt-Out Period, Customer may not terminate the Agreement, and Customer will pay any invoice(s) for the remainder of the Term, Net 45.

Hardware and Software Products

Annual recurring amounts over subscription term

Item	Cost	Quantity	Total
Flock Safety Platform			**$30,000.00**
Flock Safety Flock OS			
FlockOS ™ - Essentials	Included	1	Included
Flock Safety LPR Products			
Flock Safety LPR, fka Falcon	Included	10	Included

Professional Services and One Time Purchases

Item	Cost	Quantity	Total
One Time Fees			
Flock Safety Professional Services			
Professional Services - Standard Implementation Fee	$650.00	10	$6,500.00

Subtotal Year 1:	$36,500.00
Annual Recurring Subtotal:	$30,000.00
Estimated Tax:	$0.00
Contract Total:	$36,500.00

Taxes shown above are provided as an estimate. Actual taxes are the responsibility of the Customer. 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.

The Term for Flock Hardware shall commence upon first installation and validation, except that the Term for any Flock Hardware that requires self-installation shall commence upon execution of the Agreement. In the event a Customer purchases more than one type of Flock Hardware, the earliest Term start date shall control. In the event a Customer purchases software only, the Term shall commence upon execution of the Agreement.

Docusign Envelope ID: D81128EE-7794-47ED-8B68-B883057EBADE

Billing Schedule

Billing Schedule	Amount (USD)
Year 1	
At PPI End Date	$36,500.00
Annual Recurring after Year 1	$30,000.00
Contract Total	$36,500.00

*Tax not included

Docusign Envelope ID: D81128EE-7794-47ED-8B68-B883057EBADE

Product and Services Description

Flock Safety Platform Items	Product Description
FlockOS ™ - Essentials	An integrated public safety platform that detects, centralizes and decodes actionable evidence to increase safety, improve efficiency, and connect the community.
Flock Safety LPR, fka Falcon	Law enforcement grade infrastructure-free (solar power + LTE) license plate recognition camera with Vehicle Fingerprint ™ technology (proprietary machine learning software) and real-time alerts for unlimited users.
Professional Services - Standard Implementation Fee	One-time Professional Services engagement. Includes site and safety assessment, camera setup and testing, and shipping and handling in accordance with the Flock Safety Standard Implementation Service Brief.

FlockOS Features & Description

FlockOS Features	Description
Community Network Access	The ability to request direct access to feeds from privately owned Flock Safety LPR cameras located in neighborhoods, schools, and businesses in your community, significantly increasing actionable evidence that clears cases.
Unlimited Users	Unlimited users for FlockOS
State Network (License Plate Lookup Only)	Allows agencies to look up license plates on all cameras opted into the Flock Safety network within your state.
Nationwide Network (License Plate Lookup Only)	With the vast Flock Safety sharing network, law enforcement agencies no longer have to rely on just their devices alone. Agencies can leverage a nationwide system boasting 10 billion additional plate reads per month to amplify the potential to collect vital evidence in otherwise dead-end investigations.
Time & Location Based Search	Search full, partial, and temporary plates by time at particular device locations
License Plate Lookup	Look up specific license plate location history captured on Flock devices
Vehicle Fingerprint Search	Search footage using Vehicle Fingerprint™ technology. Access vehicle type, make, color, license plate state, missing / covered plates, and other unique features like bumper stickers, decals, and roof racks.
Insights & Analytics	Reporting tool to help administrators manage their LPR program with device performance data, user and network audits, plate read reports, hot list alert reports, event logs, and outcome reports.
ESRI Based Map Interface	Map-based interface that consolidates all data streams and the locations of each connected asset, enabling greater situational awareness and a common operating picture.
Real-Time NCIC Alerts on Flock ALPR Cameras	Receive automated alerts when vehicles entered into established databases for missing and wanted persons are detected, including the FBI's National Crime Information Center (NCIC) and National Center for Missing & Exploited Children (NCMEC) databases.
Unlimited Custom Hot Lists	Ability to add a suspect's license plate to a custom list and get alerted when it passes by a Flock camera
Law Enforcement Network Access	The ability to request direct access to evidence detection devices from Law Enforcement agencies outside of your jurisdiction.

Docusign Envelope ID: D81128EE-7794-47ED-8B68-B883057EBADE

By executing this Order Form, Customer represents and warrants that it has read and agrees all of the terms and conditions contained in the Terms of Service located at https://www.flocksafety.com/terms-and-conditions

The Parties have executed this Agreement as of the dates set forth below.

FLOCK GROUP, INC.

By: Signed by: Mark Smith AC5C931454C24F3...

Name: Mark Smith

Title: General Counsel

Date: 3/17/2025

Customer: MI - Pentwater PD

By: Signed by: Laude Hartrum DD06A42CF2D9458...

Name: Laude Hartrum

Title: Chief of Police

Date: 3/17/2025

PO Number: _____

Terms and Conditions

Agreements and Policies

Terms and Conditions

Privacy Policy

License Plate Reader Policy

Trademark Notice

API and Integrations Terms

Flock Evidence Policy

State-Specific Contractual Provisions

Vendor Information Security Addendum

Vendor Data Processing Addendum

Vendor Downstream Subcontractor Business Associate Addendum

Vendor Compliance Addendum

Part 91 Operational Agreement for Quality Checks, Quality Assurance, and Maintenance

Product Specific Terms

Third Party Terms

Vulnerability Disclosure Policy

Customer InfoSec Addendum

Last Updated: August 21, 2026

To access prior versions of Flock's online Customer Terms & Conditions, click HERE

To access Flock's Plain English explanation of Customer Data ownership, click HERE

1. DEFINITIONS

1.1. "Agreement" means these Terms and Conditions, any exhibits attached hereto, the Reinstall Fee Schedule, the Customer Implementation Guide, the InfoSec Addendum, the State Specific Terms, the Product Specific Terms, the Third Party Terms, and each Order Form, each of which is incorporated by reference.

1.2. "Applicable Law" means all federal, state, and local laws and regulations, including those related to the recording or sharing of data, video, photo, or audio content, in each case to the extent directly applicable to the respective Party's performance of its obligations under this Agreement.

1.3. "Authorized End User(s)" means any individual employees, agents, or contractors of Customer accessing or using the Flock Services on behalf of Customer pursuant to the Agreement, who have been (a) granted access to the Flock Services by Customer in its exercise of

Data Ownership

Security Advisories

reasonable discretion relating to the receipt of the Flock Services hereunder by Customer, and (b) from whom Customer has obtained reasonable assurances that they will comply with the access and use and confidentiality terms in the Agreement.

1.4. "Confidential Information" means information that is disclosed by one Party to the other and that the receiving Party knows is confidential to the disclosing Party or that is of such a nature that someone familiar with the type of business of the disclosing Party would reasonably understand is confidential to it. Confidential Information includes financial, product, and other business information of either Party. With respect to Customer, Confidential Information includes Customer Data. Notwithstanding the foregoing, Confidential Information does not include information that the receiving Party can demonstrate: (a) is in the public domain or is generally publicly known through no improper action or inaction by the receiving Party; (b) was rightfully in the receiving Party's possession or known by it prior to receipt from the disclosing Party; (c) is rightfully disclosed without restriction to the receiving Party by a third-party without violation of obligation to the disclosing Party; or (d) is independently developed for the receiving Party by third parties without use of the Confidential Information of the disclosing Party.

1.5. "Customer" means the entity identified in the signature block of the Order Form to which these Terms & Conditions apply.

1.6. "Customer Data" means all (a) data and information captured by Flock Hardware on behalf of Customer through the Flock Services (e.g., images, audio, and/or video) and metadata associated therewith, (b) content input into the Web Interface by Customer or its Authorized End Users, and (c) data and information provided to Flock through the Flock Services by third parties at Customer's direction.

1.7. "Customer Hardware" means the third-party hardware owned or otherwise provided by Customer, and any other

physical elements that interact with the Flock Software to provide the Flock Services.

1.8. "Customer Implementation Guide" means the terms and conditions related to implementation located at https://www.flocksafety.com/implementation-guide.

1.9. "Effective Date" means the date the applicable Order Form is executed by both Parties.

1.10. "Feedback" means any ideas, advice, recommendations, suggestions, enhancement requests, feedback, or proposals provided by, or on behalf of, Customer or its personnel to Flock related to Flock Property.

1.11. "Flock Hardware" means all Flock device(s) and physical elements provided by Flock in connection with the Flock Services.

1.12. "Flock Property" means the Flock Services, the Flock Software, Flock Hardware, the Web Interface, Flock's Confidential Information, and all intellectual property or proprietary information therein or otherwise provided to Customer or its Authorized End Users, including Flock's technology, patents, trade secrets, trademarks, proprietary methods, algorithms, data models, machine learning methods, documentation, and any modifications or improvements. For clarity, Flock Property also includes any derivative works, intermediate or final outputs, analyses, reports, models, or other results generated by or through the Flock Services. Except for the limited ability to access and download Customer Data within the applicable Retention Period, no rights are granted to download, extract, export, or otherwise create or retain copies of such derivative works, outputs, or other elements of Flock Property.

1.13. "Flock Services" means the services provided by Flock under the Agreement as set forth in the applicable Order Form, including access to and use of the Web

Interface by Customer and the provision of Flock Software and Flock Hardware.

1.14. "Flock Software" means the (a) software and/or firmware integrated with or installed on the Flock Hardware or Customer Hardware; and (b) the software functionality of the Web Interface that enables system access and use.

1.15. "Force Majeure Event" means, with respect to a Party, any event or circumstance, whether or not foreseeable, that was not caused by that Party and any consequences of that event or circumstance.

1.16. "InfoSec Addendum" means the Customer Information Security Addendum located at https://www.flocksafety.com/legal.

1.17. "Order Form" means any Flock Order Form entered into by the Parties on the date hereof or following the Effective Date and incorporated herein by reference. Each Order Form will describe the Flock Services to be performed and the period for performance.

1.18. "Permitted Purpose" means a legitimate public safety and/or business purpose, including the awareness, prevention, and prosecution of crime; investigations; and prevention of commercial harm, to the extent permitted by law.

1.19. "Product Specific Terms" means the product-specific terms and conditions related to the Flock Services utilized by Customer located at https://www.flocksafety.com/legal.

1.20. "Reinstall Fee Schedule" means the fee schedule set forth at https://www.flocksafety.com/reinstall-fee-schedule.

1.21. "Retention Period" means the time period that footage captured by the Flock Hardware or Customer Hardware via the Flock Services and the associated metadata is stored by Flock, as specified in the applicable Order Form.

1.22. "State Specific Terms" means the state-required terms located at https://www.flocksafety.com/legal applicable to Customers located in the state(s) set forth therein.

1.23. "Third Party Items" means the third party products and services accessible to Customer through the Flock Services.

1.24. "Third Party Terms" means the pass-through terms and conditions set forth at https://www.flocksafety.com/legal applicable to Customer's access to and use of certain Third Party Items.

1.25. "Web Interface" means the website(s) or application(s) through which Customer and its Authorized End Users can access the Flock Services.

2. ACCESS AND USE

2.1. Provision of Access. Subject to compliance with the terms of the Agreement, Flock grants to Customer and its Authorized End Users a limited, non-exclusive, non-transferable right to access and use the Flock Services via the Web Interface during the term of this Agreement, solely for the Permitted Purpose. Customer shall access the Flock Services through the Web Interface only (a) through its Authorized End Users acting within the scope of their service for Customer; (b) for the internal use of Customer; and (c) from and within the United States.

2.2. Authorized End Users. Authorized End Users (i) agree to provide Flock with accurate, complete, and updated registration information; (ii) may not select as their User ID, a name that they do not have the right to use, or any other name with the intent of impersonation; (iii) shall not share their account username or password information and must protect the security of the username and password; and (iv) shall only use Customer-issued email addresses for the creation of their User ID. Customer and Authorized End Users may not transfer their account to anyone else without Flock's prior

written permission. Customer shall be responsible for all acts and omissions of Authorized End Users in connection with their access and use of the Flock Services, including each Authorized End User's compliance with the terms of the Agreement and Applicable Law. Customer shall terminate any Authorized End User's access to the Flock Services (a) when such person no longer meets the definition of "Authorized End User;" (b) if conduct by such Authorized End User breaches any term of the Agreement; or (c) upon such Authorized End User's indictment, arrest, or conviction for any felony offense. Flock may restrict, suspend, or terminate an Authorized End User's access to the Flock Services if Flock determines, in its reasonable discretion, that such access has an adverse effect on Flock or any of its customers. Customer is responsible for any use of data, information, or services obtained through the Flock Services by Authorized End Users.

2.3. Access and Use Restrictions. Except as expressly permitted under the Agreement, Customer and its Authorized End Users shall not: (a) access or use Flock Property in connection with the provision of any services to third parties; (b) resell, rent, license, lease, transfer, encumber, copy, distribute, publish, exhibit, transmit or otherwise make available to any third-party any Flock Property; (c) derive specifications from, reverse engineer, reverse compile, disassemble, translate, record, or create derivative works based on Flock Property; (d) use Flock Property in a manner that delays, impairs, or interferes with system functionality for others or that compromises the security or integrity of any data, equipment, software, or system input or output, including introduction of any viruses or malware into the Web Interface; (e) use Flock Property or any part or aspect thereof in violation of Applicable Law or to mislead, harass, stalk, or otherwise impose upon or violate the rights of any person; or (f) otherwise use Flock Property, except as specifically permitted under the Agreement. Use of, or access to, Flock Property not in accordance with the terms of the Agreement is strictly prohibited. Any violation of this Section 2 will cause Flock irreparable and immediate harm, entitling Flock to injunctive

relief to prevent such violation. In the event of a reasonably suspected violation of this Section 2.3, Flock may temporarily suspend Customer and/or any Authorized End User's access to any portion or all of the Flock Property (a "Service Suspension"). Customer shall not be entitled to any remedy for any Service Suspension imposed in accordance with the Agreement, including any reimbursement, tolling, or credit.

3. SERVICES AND SUPPORT

3.1. Support Services. Flock shall monitor the Flock Services, and any applicable device health, in order to improve performance and functionality. Flock will use commercially reasonable efforts to respond to requests for support within seventy-two (72) hours. Flock will provide Customer with reasonable technical and on-site support and maintenance services in-person, via phone, or by email at support@flocksafety.com (such services collectively referred to as "Support Services").

3.2. Service Disruptions. Access to the Web Interface may be disrupted in the event that: (a) Flock's provision of the Flock Services to Customer or any Authorized End User is prohibited by Applicable Law; (b) any third-party services required for Flock's provision of the Flock Services are interrupted; (c) the Flock Services are being used for malicious, unlawful, or otherwise unauthorized purposes; (d) there is a threat or attack on any Flock Property by a third-party; or (e) there is scheduled or emergency maintenance ("Service Disruption"). Flock will make commercially reasonable efforts to provide written notice of any Service Disruption to Customer, to provide updates, and to resume providing access to the Web Interface as soon as reasonably possible after the event giving rise to the Service Disruption. To the extent the Service Disruption is not caused by Customer or its Authorized End Users' direct actions or omissions, the term of the Flock Services affected by such Service Disruption will be tolled by the duration of the Service Disruption for any continuous disruption lasting at least one (1) full day. For example, in the event of a Service Disruption lasting five (5) continuous

format, or transmission method outside of the Web Interface. To the extent any Customer Data constitutes personal data or personal information (as defined under Applicable Laws), Flock will process such data in accordance with Applicable Law and the privacy policy set forth at https://www.flocksafety.com/legal/privacy-policy. Flock will comply with its obligations under the InfoSec Addendum.

4.2. Flock Property. Except for the right to use Flock Property subject to the terms and conditions contained herein, the Agreement does not confer on Customer a license in, ownership of, or interest in Flock Property. Flock developed or acquired Flock Property exclusively at its private expense. As between the Parties, Flock Property and all right, title, and interest in and to it is and will remain the exclusive property of Flock.

5. CONFIDENTIALITY. Each Party shall exercise reasonable care to hold Confidential Information in confidence and not use it or disclose it to any other person or entity, except (a) as permitted under this Agreement or as reasonably necessary for the performance or enforcement of this Agreement; (b) as agreed in writing by the other Party; (c) for the Party's proper management and administration (provided that it obtains reasonable assurances from all recipients that they will keep the information confidential and use it only for the purpose of its disclosure; and provided further that it is responsible for all acts and omissions of any such recipient in violation of this Section 5); or (d) as required by law, including in response to any valid legal process, provided that receiving Party shall, to the extent permissible, give the disclosing Party reasonable prior notice of such disclosure. Any violation of this Section 5 may cause the non-violating Party irreparable and immediate harm, and such Party is entitled to injunctive relief to prevent such violation. Upon termination of this Agreement, at Customer's request, all Confidential Information will be deleted within 90 days. Flock will not be required to delete any data which it is obligated to retain pursuant to an applicable legal obligation or policy (e.g., inter-agency audit log integrity or metadata held for evidentiary

days, Customer will receive a credit for five (5) free days at the end of the term of the applicable Order Form. The remedy of a credit described in this Section 3.2 will be Customer's sole and exclusive remedy for the acts or omissions of Flock relating to such Service Disruption.

3.3. Product Specific Terms. The Parties will comply with their obligations set forth in the Product Specific Terms applicable to the Flock Services utilized by Customer.

3.4. Third Party Items. As applicable in connection with the Flock Services, Flock hereby grants to Customer and its Authorized End Users a limited, non-exclusive, non-transferable, non-licensable right to access and use the Third Party Items through the Flock Services during the term of this Agreement. Flock may modify the Third Party Terms in the event Flock adds or replaces Third Party Items or as required in connection with changes to the applicable third party agreements for the Third Party Items. The Third Party Items will not be deemed part of Flock Property.

4. DATA USE AND LICENSING

4.1. Customer Data. As between Flock and Customer, all right, title, and interest in and to Customer Data belong to and are retained by Customer. Customer hereby grants to Flock a limited, non-exclusive, royalty-free, irrevocable, perpetual, worldwide license to (a) use and disclose Customer Data to provide the Flock Services; and (b) use Customer Data to support and improve Flock's products and services. For the avoidance of doubt, Flock shall not sell Customer Data. Any sharing by Flock of Customer Data that is not (i) specifically permitted by this Agreement, or (ii) separately directed and/or authorized by Customer, shall constitute a prima facie breach of this Agreement, and Customer shall be entitled to all remedies available to it under this Agreement and the law. Customer Data will be available for Authorized End Users to access and download via the Web Interface during the applicable Retention Period. Flock is not obligated to provide Customer Data in any alternative form,

authentication), provided that Flock shall ensure the confidentiality of such Confidential Information for so long as it is retained.

6. PAYMENT OF FEES

6.1. Billing and Payment of Fees. Customer shall pay the fees set forth in the applicable Order Form based on the billing structure and payment terms as indicated in the Order Form. To the extent the Order Form is silent, Customer shall pay all invoices thirty (30) days from the date of each such invoice. If Customer believes that Flock has billed Customer incorrectly, Customer must contact Flock no later than thirty (30) days following the date of the first invoice in which the error or problem appeared to receive an adjustment or credit. Customer acknowledges and agrees that a failure to contact Flock within this period will serve as a waiver of any claim. If any undisputed fee is more than thirty (30) days overdue, Flock may, without limiting its other rights and remedies, suspend delivery of the Flock Services until such undisputed invoice is paid in full. Flock shall provide at least thirty (30) days' prior written notice to Customer of the payment delinquency before exercising any suspension right. Customer shall direct all queries regarding billing or payment concerns to support@flocksafety.com. Flock may impose a late fee equal to the lesser of (a) 1.5%, or (b) the highest rate permitted by Applicable Law, each month on all amounts overdue beyond ten (10) days, but this charge will not waive or extend any obligation of Customer to make payments when due.

6.2. Notice of Changes to Fees. In the event of any changes to fees, Flock shall provide Customer with sixty (60) days' notice (email sufficient) prior to the end of the term of the applicable Order Form. Any such changes to fees shall only impact subsequent renewal terms.

6.3. Taxes. Customer is responsible for all taxes, levies, or duties, excluding only taxes based on Flock's net income, imposed by taxing authorities associated with the order. If Flock has the legal obligation to pay or collect taxes, including amounts subsequently assessed by a taxing

authority, for which Customer is responsible, the appropriate amount shall be invoiced to and paid by Customer unless Customer provides Flock a legally sufficient, valid tax exemption certificate authorized by the appropriate taxing authority. Flock shall not charge Customer any taxes from which it is exempt. If any deduction or withholding is required by law, Customer shall notify Flock and shall pay Flock any additional amounts necessary to ensure that the net amount that Flock receives, after any deduction and withholding, equals the amount Flock would have received if no deduction or withholding had been required.

7. TERM AND TERMINATION

7.1. Term. These Terms & Conditions will be effective from the Effective Date and will continue in full force and effect until terminated as set forth herein. The term of each Order Form will be as set forth therein.

7.2. Termination. Upon termination or expiration of the Agreement or any applicable Order Form, Flock will remove any applicable Flock Hardware within a commercially reasonable time period. Either Party may terminate this Agreement effective upon written notice to the other Party if (a) the other Party defaults in performance of any material provision of the Agreement and such default is not cured within thirty (30) days following written notice describing the specific default; (b) the other Party violates Applicable Law; (c) the other Party files a voluntary petition in bankruptcy or an involuntary petition is filed against it; (d) the other Party is adjudged bankrupt; (e) a court assumes jurisdiction of the assets of the other Party under a federal reorganization act or other statute; (f) a trustee or receiver is appointed by a court for all or a substantial portion of the assets of the other Party; (g) the other Party becomes insolvent, suspends business, or ceases to conduct its business in the ordinary course; (h) the other Party makes an assignment of its assets for the benefit of its creditors; or (i) there are no active Order Forms under these Terms & Conditions. In the event Customer terminates the Agreement pursuant to Section 7.2(a), Flock will refund

Customer a pro-rata portion of the pre-paid fees for the Flock Services not received prior to the date of termination.

7.3. Survival. The following Sections will survive termination: 1, 4, 5, 6, 7, 8.5, 9, and 11.

7.4. Payment Upon Termination. Upon termination of the Agreement or any Order Form for any reason, Customer shall pay to Flock all amounts due hereunder for all Flock Services rendered through the date of termination in accordance with the terms of the Agreement.

8. REPRESENTATIONS AND WARRANTIES

8.1. Manufacturer Defect. Upon a malfunction or failure of Flock Hardware (a "Defect"), Customer must notify Flock's technical support team. Flock shall conduct an inspection or test any Customer-reported Defect within seven (7) business days of notification, and Flock shall use commercially reasonable efforts to repair or replace, in Flock's sole discretion, the defective Flock Hardware at no additional cost to Customer.

8.2. Flock Representations and Warranties. Flock represents and warrants to Customer that (a) the Flock Services, when used in accordance with the Agreement and as expressly authorized by Flock, do not infringe any valid patent, registered copyright, or other registered intellectual property right under the laws of the United States, provided that Flock makes no warranty to the extent such infringement results from (i) use of the Flock Services by Customer in combination with any data, software, or equipment not provided by Flock, where such infringement would have been avoided absent such combination, or (ii) any breach of the Agreement by, or any negligent or other wrongful act or omission of, Customer or any party acting on Customer's behalf; (b) Flock's personnel will perform the Flock Services in a professional and workmanlike manner, consistent with generally accepted industry standards; and (c) Flock's personnel performing the Flock Services will be appropriately trained for their assigned roles and

will perform the Flock Services in all material respects in accordance with prevailing industry standards.

8.3. Customer Representations and Warranty. Customer represents and warrants to Flock that (a) Customer shall access and use the Flock Services only in compliance with the Agreement, the Permitted Purpose, and Applicable Law; (b) Customer has all rights, permissions, and authorizations necessary to provide Customer Data to Flock and to direct Flock to collect, use, and otherwise handle Customer Data as contemplated by the Agreement; and (c) Customer will obtain and maintain any notices, signage, or consents required in connection with Customer's deployment, configuration, access to, sharing of, and use of the Flock Services and Customer Data.

8.4. Mutual Representations and Warranties. Each Party represents and warrants to the other Party that (a) it has the requisite corporate power and authority to execute and perform its obligations under the Agreement; (b) the person executing the Agreement on its behalf has the authority to bind it hereunder and that such Party's execution of the Agreement is not in violation of such Party's bylaws, certificate of incorporation, or other comparable document; (c) the execution, delivery, or performance of the Agreement will not violate or conflict with, require consent under, or result in any breach or default of (i) Applicable Law, or (ii) any covenants or agreements by which such Party or any of its assets are bound; and (d) each Party will comply with Applicable Law.

8.5. Disclaimer. THE REMEDY DESCRIBED IN SECTION 8.1 ABOVE IS CUSTOMER'S SOLE AND EXCLUSIVE REMEDY, AND FLOCK'S SOLE LIABILITY, WITH RESPECT TO DEFECTS. FLOCK DOES NOT WARRANT THAT THE FLOCK 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 FLOCK SERVICES. EXCEPT AS EXPRESSLY SET FORTH IN THIS SECTION 8, THE FLOCK SERVICES ARE PROVIDED "AS IS," AND FLOCK DISCLAIMS ALL

REPRESENTATIONS AND WARRANTIES OF ANY KIND OR NATURE, EXPRESS OR IMPLIED (EITHER IN FACT OR BY OPERATION OF LAW), WITH RESPECT TO ANY SERVICE OR ITEM PROVIDED HEREUNDER. THIS SECTION 8.5 APPLIES TO THE EXTENT PERMITTED BY LAW.

8.6. Insurance. Flock will maintain the insurance policies set forth on Exhibit A attached hereto.

9. LIMITATION OF LIABILITY. FLOCK'S CUMULATIVE, AGGREGATE LIABILITY IN CONNECTION WITH, OR ARISING IN ANY WAY OR IN ANY DEGREE FROM, THE AGREEMENT, FROM THE FLOCK SERVICES, OR OTHERWISE FROM THE ACTS OR OMISSIONS OF FLOCK WILL NOT EXCEED THE TOTAL AMOUNT PAID BY CUSTOMER TO FLOCK IN THE TWELVE (12) MONTHS BEFORE SUCH CLAIM AROSE. NOTWITHSTANDING ANYTHING TO THE CONTRARY, FLOCK WILL NOT BE LIABLE FOR INDIRECT, EXEMPLARY, PUNITIVE, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OR LOSSES; ADDITIONAL OVERHEAD AND PAYROLL; LOST PROFITS OR BUSINESS OPPORTUNITIES; LOSS OF DATA; OR THE COST OF PROCUREMENT OF SUBSTITUTE ITEMS OR SERVICES. THIS SECTION 9 APPLIES TO THE EXTENT PERMITTED BY LAW. Customer hereby acknowledges that the remedies set forth above are reasonable.

10. FLOCK HARDWARE (APPLICABLE ONLY WHERE CUSTOMER HAS LICENSED FLOCK HARDWARE)

10.1. Flock Hardware. Customer is not permitted to remove, reposition, re-install, tamper with, alter, adjust, or otherwise take possession or control of Flock Hardware. In the event Customer is found to engage in any of the foregoing restricted actions, all warranties herein shall be null and void, and Flock shall be entitled to terminate the Agreement in accordance with Section 7.2(a). Customer shall not perform any acts which would interfere with Flock's retention of title to the Flock Hardware. Should Customer default on any payment of the Flock Services, Flock may immediately cut off access to the Web Interface and remove Flock Hardware at Flock's

discretion. Such actions, if made by Flock, shall not be deemed a waiver of Flock's rights to any damages Flock may sustain as a result of Customer's default, and Flock shall have the right to enforce any other legal remedy or right.

10.2. Deployment Plan. Flock shall advise Customer on the location and positioning of the Flock Hardware for optimal product functionality, as conditions and locations allow. Flock will collaborate with Customer to design the strategic geographic mapping of the location(s) and implementation of Flock Hardware to create a deployment plan associated with each Order Form (each, a "Deployment Plan"). In the event that Flock determines that Flock Hardware will not achieve optimal functionality at a designated location, Flock shall have final discretion to veto a specific location and will provide alternative options to Customer. After installation of Flock Hardware, any subsequent requested changes to the Deployment Plan, including relocating, re-positioning, adjusting of the mounting, removing foliage, replacement, and/or changes to heights of poles will incur a fee as set forth in the Reinstall Fee Schedule. Customer will receive prior notice and confirm approval of any such fees.

10.3. Customer Installation Obligations. Customer is responsible for any applicable supplementary cost as described in the Customer Implementation Guide. Customer represents and warrants that it has, or shall lawfully obtain, all necessary rights and authority and hereby authorizes Flock to install the Flock Hardware at the designated locations and to make any necessary inspections or maintenance in connection with such installation.

10.4. Replacements In the event that Flock Hardware is lost, stolen, or damaged, Customer may request a replacement of Flock Hardware at a fee as set forth in the Reinstall Fee Schedule. In the event Customer chooses not to replace lost, stolen, or damaged Flock Hardware, Flock shall not be liable for any resulting impact to the Flock Services, nor shall Customer receive a refund for the lost, damaged, or stolen Flock Hardware.

10.5. Hazardous Conditions. Flock Services do not contemplate hazardous materials or other hazardous conditions, including, without limit, asbestos, lead, or 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 the Agreement, Flock shall have the right to cease work immediately.

11. MISCELLANEOUS

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

11.2. Assignment. Neither Party may assign the Agreement or any right under the Agreement, in each case by operation of law or otherwise, except as otherwise permitted hereunder without the prior written consent of the other Party, and any attempt to assign the Agreement or any right under the Agreement in breach of the provisions of this Section 11.2 shall be null and void. The foregoing notwithstanding, either Party may assign the Agreement upon written notice to the other Party in connection with (a) any reorganization, conversion, consolidation or merger of such Party, (b) any transaction resulting in the holders (together with their affiliates) of a majority of the voting securities, membership interest or right to appoint a majority of the members of the board of directors or similar governing body of such Party as of immediately prior to such transaction, holding less than such a majority as of immediately after such transaction, or (c) any sale, transfer or exclusive license of all or a majority of the assets of such Party that are pertinent to the Agreement or, in each case of (a) through (c) whether consummated in one transaction or a series of related transactions. For the avoidance of doubt, the assigning Party and the assignee will remain liable jointly and severally for any unperformed obligations under the Agreement or any breach hereof arising prior to the effective date of any assignment of the Agreement. The Agreement is

binding on the Parties and their successors and permitted assigns.

11.3. Entire Agreement. The Agreement constitutes the entire agreement between the Parties relating to the Flock Services and supersedes all prior agreements, understandings, and representations relating to the Flock Services. No waiver or modification to the Agreement will be effective or binding unless signed by Customer and a duly authorized representative of Flock, except as otherwise provided herein. None of Customer's purchase orders, questionnaires, portal terms and conditions, authorizations, or similar documents will alter the terms of the Agreement or be binding upon Flock, and any such terms are expressly rejected. Any mutually agreed purchase order is subject to the terms of the Agreement. Customer agrees that Customer's purchase is neither contingent upon the delivery of any future functionality or features nor dependent upon any oral or written comments made by Flock with respect to future functionality or feature.

11.4. Relationship. The Parties intend that nothing contained in the Agreement be construed to create an agency, partnership, joint venture, employment, or like relationship between the Parties, and their relationship is and will remain that of independent Parties to a contractual service relationship. Neither Party will be liable for the debts or obligations of the other Party.

11.5. Governing Law; Dispute Resolution. The Agreement, and any controversy or claim arising out of or relating to the Agreement (each, a "Dispute") shall be governed exclusively by, and construed and enforced in accordance with, the laws of the State of Georgia, without regard to its conflicts of laws principles. If any Dispute cannot be settled through direct discussions, the Parties agree to endeavor first to settle such Dispute by mediation administered by the American Arbitration Association under its Commercial Mediation Procedures before resorting to arbitration. The Parties further agree that any Dispute that remains unresolved by mediation

shall be settled by arbitration administered by the American Arbitration Association in accordance with its Commercial Arbitration Rules and judgment on the award rendered by the arbitrator(s) may be entered in any court having jurisdiction thereof. The Parties agree that the United Nations Convention for the International Sale of Goods is excluded in its entirety from this Agreement.

11.6. Publicity. Flock will obtain Customer's consent before using Customer's name or logo in a manner signifying an endorsement of Flock by Customer; provided, however that Flock may refer to Customer as a current customer without first obtaining Customer's consent.

11.7. Feedback. Any Feedback: (a) is given to Flock without claim of intellectual property right by Customer, (b) by its receipt grants Flock a royalty free, worldwide, transferable, sub-licensable, irrevocable, perpetual license to commercialize, use, and incorporate such Feedback into its software, services, or systems, or use as it otherwise deems necessary or desirable in its business, and (c) will not enable Customer to claim any interest in or ownership of Flock Property.

11.8. Export. Customer may not remove or export from the United States or allow the export or re-export of Flock Property 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 Customer or authority. As defined in Federal Acquisition Regulation ("FAR"), section 2.101, the Flock Services, Flock Hardware, and documentation are "commercial items" 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 the Agreement and will be prohibited except to the extent expressly permitted by the terms of the Agreement.

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

11.10. Conflict. To the extent of a conflict between the Agreement and any applicable statement of work or mutually-agreed purchase order, the Agreement controls unless explicitly stated otherwise. From time to time, the Parties may mutually agree in a signed Order Form to certain special terms applicable to such Order Form ("Special Terms"). To the extent of any conflict or inconsistency between or among the terms of these Terms & Conditions, the terms of any Order Form (excluding Special Terms), or the Special Terms themselves, the order of priority (from highest to lowest) in which the respective documents will govern to the extent of such conflict or inconsistency shall be as follows: (i) the Special Terms; (ii) these Terms & Conditions; and (iii) the Order Form (excluding Special Terms).

11.11. Notices. All notices under the 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. All notices will be provided to the email or mailing address listed in the Order Form.

11.12. Non-Appropriation. All obligations of the Customer under the Agreement which require

the expenditure of public funds are conditioned on the availability of said funds appropriated for that purpose. To the extent applicable, if funds are not appropriated for a future fiscal year, Customer shall have the right to terminate the Agreement for non-appropriation at the end of the applicable fiscal year upon thirty (30) days' written notice to Flock. Customer shall remain responsible for all amounts incurred prior to termination.

11.13. Construction. When used in the Agreement, "including" means "including without limitation."

11.14. Force Majeure.

11.14.1. If a Force Majeure Event prevents a Party from complying with any one or more obligations under the Agreement, that inability to comply will not constitute breach if (a) that Party uses reasonable efforts to perform those obligations; (b) that Party's inability to perform those obligations is not due to its failure to (i) take reasonable measures to protect itself against events or circumstances of the same type as that Force Majeure Event, or (ii) develop and maintain a reasonable contingency plan to respond to events or circumstances of the same type as that Force Majeure Event; and (c) that Party complies with its obligations under Section 11.14.2.

11.14.2. During a Force Majeure Event, the noncomplying Party shall use reasonable efforts to limit damages to the other Party and to resume its performance under the Agreement.

11.15. Third Parties. Except as explicitly set forth herein, none of the provisions of the Agreement will be for the benefit of or enforceable by any third-party.

11.16. Waivers. No failure by a Party to insist upon the strict performance of any term or condition of the Agreement or to exercise any right or remedy hereunder will constitute a waiver.

11.17. Execution. In connection with the Flock Services, a copy of a signed document sent by PDF or fax will be deemed an original in the hands of the recipient. The Agreement may be executed in counterparts and exchanged by electronic means, each of which shall be deemed an original, and both of which together constitute only one agreement between the Parties.

EXHIBIT A

INSURANCE

1. Required Coverage. Flock shall procure and maintain for the duration of the Agreement insurance against claims for injuries to persons or damages to property that may arise from or in connection with the performance of the services under the Agreement and the results of that work by Flock or its agents, representatives, employees, or subcontractors. Insurance shall be placed with insurers with a current A. M. Best rating of no less than "A" and "VII". Flock shall obtain and, during the term of the Agreement, shall maintain policies of professional liability (errors and omissions), automobile liability, and general liability insurance for insurable amounts of the limits listed herein. The insurance policies shall provide that the policies shall remain in full force during the life of the Agreement. Flock shall procure and shall maintain during the life of the Agreement Worker's Compensation insurance as required by applicable State law for all Flock employees. For the avoidance of doubt, (a) all required insurance limits by Customer can be met through a combination of primary and excess/umbrella coverage, and (b) Flock's Cyber and Professional Liability/Errors and Omissions insurance has a shared limit of Five Million Dollars (5,000,000) per incident and in the aggregate.

2. Types and Amounts Required. Flock shall maintain the following insurance coverage for the duration of the Agreement:

(a) Commercial General Liability insurance written on an occurrence basis with limits of One

Million Dollars ($1,000,000) per occurrence and Two Million Dollars ($2,000,000) in the aggregate for bodily injury, death, and property damage, including personal injury, liability assumed under an insured contract, independent contractors, broad-form property damage, and product and completed operations coverage;

(b) Workers Compensation insurance in accordance with statutory limits;

(c) Professional Liability/Errors and Omissions insurance with limits of Five Million Dollars ($5,000,000) each claim and in the aggregate;

(d) Commercial Automobile Liability insurance with a combined single limit of One Million Dollars ($1,000,000) per occurrence for bodily injury, death, and property coverage, including owned and non-owned and hired automobile coverage; and

(e) Cyber Liability insurance written on a per claim basis with limits of Five Million Dollars ($5,000,000).

Submitted Public Comments

Outlook

Flock Cameras

From John Wallace [redacted]
Date Mon 9/28/2026 7:58 AM
To Laude Hartrum <lhartrum@pentwatervillage.org>

I don't feel that Flock cameras are necessary in the Village of Pentwater.
What 900 residents? We have very little crime.
Additionally, the cost of the Flock cameras is excessive.
Sincerely,
John Wallace
[redacted]
Pentwater

Sent from my iPhone

Outlook

Surveillance Cameras

From Steve Bass [redacted]
Date Sun 9/27/2026 11:04 AM
To Laude Hartrum <lhartrum@pentwatervillage.org>

Hi Laude,

I understand discussions are underway as to whether or not to keep the current surveillance cameras around the village.

I'd like to add my voice/vote to the discussion and let you know I prefer to have the cameras discontinued and removed because I feel they are "off brand" for small town American living. We all come to Pentwater to enjoy the way life used to be, not to tap into a dystopian vision of the future.

I appreciate the cameras are a valuable tool for law enforcement, but I value human interaction rather than machines here. Let's leave the machines to the big cities, please.

Thanks for your consideration,

Steve Bass

Hasbas Entertainment Inc.
[redacted]
www.hasbas.com

Outlook

Concerns Regarding Proposed Flock ALPR Camera Deployment

From Josh Andrews [redacted]
Date Sun 9/27/2026 12:11 PM
To Laude Hartrum <lhartrum@pentwatervillage.org>

Dear Chief Hartrum,

Thank you for including me in the discussion about Pentwater's Flock camera deployment. I'm writing to put my concerns on the record ahead of your report to the village council.

After reviewing the available evidence, I do not support the deployment of Flock cameras in the Village of Pentwater.

My objection is not primarily about contract terms — it's about structural issues with the technology and the vendor that I don't believe any local agreement can fully resolve.

1. Data ownership and monetization

Flock's contracts state that agencies own their data, but reporting has raised questions about whether the company retains rights to use certain data for model training regardless of that framing. Before any decision is made, I'd ask that the specific data-retention and model-training clauses in any proposed contract be reviewed in detail and shared with the public, not just summarized.

2. Documented officer misuse

This is an established pattern nationally:

- A Kentucky officer was arrested after allegedly searching an ex-girlfriend's license plate over 2,000 times, caught only because Flock's own automated audit tool flagged the pattern.
- A Milwaukee officer was charged after allegedly running 179 searches on a dating partner and her ex-partner, each logged with the single word "investigation" — an analysis found "investigation" was the most common search justification used by Wisconsin agencies overall, which suggests the audit trail is often too vague to catch misuse on its own.
- A public-interest law firm tracking these cases nationally has documented at least 47 officers disciplined for using Flock to track romantic interests, and believes that number significantly understates the true scale.

Even if we have rules and standards in place for our local officers, data sharing puts Pentwater residents' data at risk from bad actors in other departments. The standards for enforcing ethical behavior have not caught up to the pace of change in this technology.

3. Data sharing beyond our community

Local deployment does not mean local control over who can access the data. I appreciate you demonstrating the sharing controls within the Flock dashboard, and I was relieved to see that you were not sharing Pentwater camera data with federal agencies. But the data sharing with agencies across the state raises concerns from a privacy perspective.

4. Lack of community support

I'd ask whether a public hearing or council vote is planned before any final decision, rather than your report serving as the extent of public discussion. If we are going to use the Flock cameras, community support and oversight is vital.

5. Capabilities beyond license plate reading

Flock's system includes capabilities beyond basic plate capture that are worth our attention:

- Its "FreeForm" tool allows searches by appearance (clothing, accessories), not just plate number.
- A September 2026 404 Media/WIRED investigation, based on a physical teardown of a Flock camera obtained from the field, confirmed the device's software explicitly detects people, not just vehicles, plates, and bicycles. This is a function Flock has not advertised. The same investigation reconstructed Flock's back-end police software and found it can identify drivers, flag vehicles that travel together repeatedly, and search by movement patterns using camera data combined with police records and commercial data.
- Flock states its systems do not currently perform facial recognition, and to date there is no evidence that they do. However, the Flock infrastructure could support that capability in the future via a software update, without new hardware or a new decision point for this community.

This matters because a vote on a small initial camera deployment is effectively a vote to join an expanding product ecosystem, not a fixed, unchanging tool.

In summary, I am grateful that you are soliciting input from the community, and I appreciate the opportunity to provide my perspective as you prepare your report.

Sincerely, Josh Andrews

Good evening,

My name is Brynn, and I live a short walk from Bass Lake in Pentwater Township. I teach high school science at Baldwin Community Schools, I bartend at the Shelby Brown Bear, I create and sell educational materials online, I waterski with the Grand City Show Skiers down in Norton Shores, and I worship at St. James Episcopalian Church in Pentwater. I'm a very busy woman, but when I learned about the Oceana County Flock camera trial, I knew I had to make the time to do something about this invasion of privacy and normalization of mass surveillance. I am writing to all of the villages of Oceana County and asking them to say NO to contracts with creepy camera companies.

I had heard of Flock cameras before, read a few news articles, but paid little attention; I was too busy, and I didn't have time to get worked up over something happening somewhere else. But then, on my drive back from the grocery store, I saw one on the exit ramp that leads to my home. It hit me at once, how this camera and its AI hive mind of other creepy cameras were tracking my movements. My movements are boring, truth be told; I go to the same handful of places over and over. So why does the Oceana County Sheriff's department need that information, and what is stopping bad actors from misusing that information, should it suit their objectives?

I did my research. Flock Safety cameras, like other automatic license plate readers, or ALPRs, are a dragnet crime fishing tool where a rod and line should suffice. Less than 1% of cars scanned by ALPRs are connected to any crime or wrongdoing.[1] Shall we place a camera facing every citizen's front door, just so we can catch criminals faking alibis? The fourth amendment protects people from unreasonable searches and seizures by the government.[2] Is it not unreasonable to track every citizen with a vehicle in this county?

In the recent Supreme Court ruling on *Chatrie v. United States*, it was ruled 6–3 that law enforcement's use of a geofence warrant to obtain a cell phone user's location history from Google constitutes a "search" under the Fourth Amendment.[3] People have a reasonable expectation of privacy in their location data, even if a third party holds that data. Does this sound familiar? Geofence warrants are subject to Fourth Amendment limitations and safeguards, such as probable cause and particularity. How far behind do you think the condemnation of ALPRs will be in this legal fight? Will we really buy into an expensive contract that may be deemed unconstitutional in a few months?

In my reading, I also learned that Flock Safety cameras aren't reliable. One in ten license plates scanned by Flock license plate readers misread the state.[1] Innocent people have been held at gunpoint by law enforcement because these creepy cameras incorrectly flagged their car as stolen.[4] Worst of all, I learned all of the ways that Flock cameras have been misused. Without proper warrants, ALPR systems have been tapped into by ICE and CBP on multiple instances in order to track and detain immigrants.[5] In Kansas, a man wrote a critical op-ed about his local police department, who then proceeded to use ALPR technology to track and pursue him starting the very day the critical piece was published.[6] In Colorado, law enforcement wrongfully accused a woman of theft based on Flock data, and then refused to look at other evidence, treating her as a convicted criminal from the moment they knocked on her door. Chrisanna Elser was put in the position of having to prove her innocence; whatever happened to the presumption of innocence?[7]

So, on the very day I saw that camera on my exit ramp, I made a protest sign out of some spare cardboard I had in my shed, I packed up a lawn chair and a cooler in my pull wagon, I put on my war armor, which, in this case, was bright red lipstick and a bright red bikini, and marched out to Oceana Drive to sit with my sign where all may see. My small action had the result I was looking for. I got *a lot* of attention. Sure, some of it was folks checking out the bikini-clad, crazy lady sunning by the road, and some of it was folks with bad eyesight misreading my "Flock OFF" sign and calling the cops, but I had many people stop their cars near me to ask about my sign. Many had never heard of Flock cameras and were appalled when I explained how they worked. A couple days later the Oceana Sheriff's department released a statement trying to calm down public unease about the cameras.

Personally, I refuse to calm down. No matter how you try to spin PR around Flock cameras, they are, by their very nature, an unethical form of mass surveillance that has proven both unreliable and easily abused. Perhaps the Oceana County Sheriff's department may argue, "We are not like those bad cops, we would never misuse this data," and maybe they wouldn't. But what about the next elected sheriff? What about the next round of deputies? And what about the other agencies that can and *do* tap into this nationwide database without warrant? Laws, court decisions, and our own decisions as a county set a precedent that can either protect citizens from or expose them to abuse by bad actors. Oceana County has an opportunity to protect its citizens, and I sincerely hope we make the most of that opportunity and say "no" to any contracts with ALPR camera companies.

Your neighbor,
Brynn

Sources:

1. https://www.aclu.org/campaigns-initiatives/get-the-flock-out
2. https://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does-fourth-amendment-mean
3. https://www.supremecourt.gov/opinions/25pdf/25-112_0am4.pdf
4. https://www.cbsnews.com/news/license-plate-readers-alpr-mistakes/
5. https://www.404media.co/ice-taps-into-nationwide-ai-enabled-camera-network-data-shows/
6. https://www.aclu.org/news/privacy-technology/tracking-alpr-cameras/alpr-against-op-ed-writer
7. https://www.cbsnews.com/colorado/news/flock-cameras-lead-colorado-police-wrong-suspect/

Tarra Anne Perez

[redacted]

Pentwater, MI 49449

[redacted]

[redacted]

Date: June 26, 2025

To:

Village of Pentwater

65 N Hancock

Pentwater, MI 49449

Subject: Cease and Desist – Unauthorized Surveillance and Violation of Constitutional Rights

To Whom It May Concern,

This letter serves as a formal cease and desist demand regarding the unauthorized use of surveillance cameras currently operating in the Village of Pentwater under a pilot test program. These cameras are reportedly on loan and are being used to monitor the public without the informed consent of its residents. I demand the immediate removal of all footage and images of myself and my private property, and the dismantling of any equipment involved in this program.

This pilot surveillance effort constitutes a violation of the Fourth Amendment of the United States Constitution, which protects citizens against unreasonable searches and seizures. It also violates Article I, Section 11 of the Michigan Constitution, which states:

The presence and operation of these cameras allow for the constant monitoring of private citizens without warrant, probable cause, or transparency. This is not only a legal violation but a moral and ethical affront to the values of personal liberty and community trust. There is no justifiable reason to implement mass surveillance in a quiet village that does not even have a stoplight or a demonstrated need for traffic or security monitoring.

As a resident, I do not consent to being part of any experimental or pilot surveillance program that erodes civil liberties. It is unacceptable for the Village to participate in the normalization of such invasive technologies under the guise of public safety, particularly when they are funded, loaned, or sponsored by external entities that have not been publicly disclosed or approved by the community at large.

Therefore, I demand the following:

1. Immediate cessation of ALL surveillance activity involving myself, my home, my minor child, or my vehicle.

2. Immediate removal and deletion of all footage, images, or data involving my likeness or property.

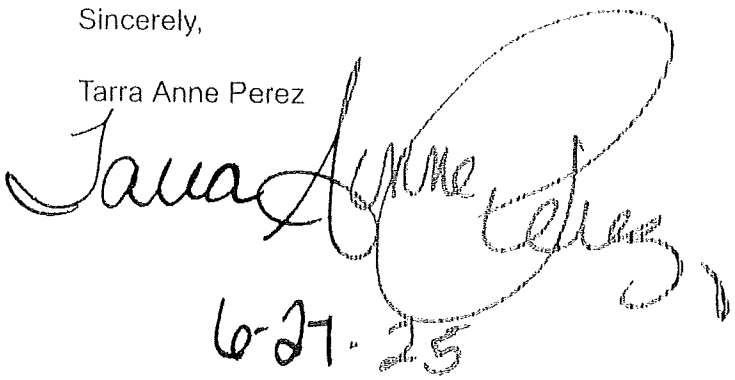
3. A formal written response within 10 business days acknowledging this letter and confirming full compliance with these demands.

Should the Village of Pentwater fail to act, I am prepared to pursue legal action in federal and state courts for constitutional violations, privacy infringement, and unlawful data collection. This may include demands for injunctive relief, compensatory damages, and legal fees.

This letter is issued without prejudice to any of my rights, all of which are fully reserved.

Sincerely,

Tarra Anne Perez



6-27-25

Proof of Service

I, Tarra Perez, declare:

On June 27, 2025, I personally delivered a true and correct copy of the attached Cease and Desist Letter to:

Recipient:

Location: Village of Pentwater Offices,

65 N Hancock

Pentwater, MI 49449

I delivered the document in the following manner (check one):

☐ In person to the above-named recipient

☒ Left with front desk staff at Village Hall

☐ Placed in official drop-box at Village Hall

I declare under penalty of perjury under the laws of the State of Michigan that the foregoing is true and correct.

Signature: Tarra Perez

Name (printed): Tarra Perez

Date: 6.27.25

Outlook

Re: 1001 Park St

From Laude Hartrum <lhartrum@pentwatervillage.org>
Date Wed 7/23/2025 12:04 PM
To Katie Saunders [redacted]
Cc Rachel Witherspoon <rwitherspoon@pentwatervillage.org>
Bcc Ryan Schiller <schillerr@oceanasheriff.net>

We will consider your comment as we move forward with the evaluation. As I'm sure your son told you the camera is not directed at your home but is focused on the Park Street.

Right now, we are tracking all the comments and questions that we get, and we are going to include them in our final evaluation this fall.

I'll keep you posted as we forward with the evaluation and work with Rachel to address your concerns.

Sorry I missed you this morning.

Chief Laude Hartrum
Pentwater Police Department
65 S Hancock Street
PO Box 622
Pentwater, Michigan 49449
Ph. 231-869-8301 #109
Cell 231-233-7633

Pentwater Police Department Confidentiality Notice

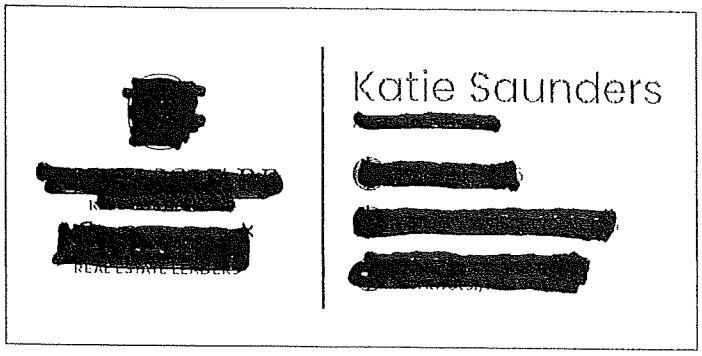
This email and any attached documents may contain confidential information, belonging to the sender, which is legally privileged. This information is intended only for the use of the individual or entity named above. The authorized recipient of this information is prohibited from disclosing this information to any other party. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is strictly prohibited. If you have received this email in error, please notify the sender immediately and delete all copies of the email from your system.

From: Katie Saunders [redacted]
Sent: Wednesday, July 23, 2025 9:08 AM
To: Rachel Witherspoon <rwitherspoon@pentwatervillage.org>
Cc: Laude Hartrum <lhartrum@pentwatervillage.org>
Subject: [redacted]

Good morning!

Thank you, Laude, for following up with my email to Rachel. I do fully understand your position on the cameras so explaining your take on them is not helpful. You know I am not one to want to make a fuzz; I just want the camera removed from across the street from my house. I think both of you and council will agree, you would also not like this outside of your home.

Sincerely,
Katie



From: Rachel Witherspoon <rwitherspoon@pentwatervillage.org>
Sent: Tuesday, July 22, 2025 3:33 PM
To: Katie Saunders [redacted]
Cc: Laude Hartrum <lhartrum@pentwatervillage.org>
Subject: Re: [redacted]

Hi Katie,

I am actually out of town this week for a conference. I am copying Chief Hartrum on this email so he can give you a more in depth explanation regarding the cameras.

Please know that they are only capturing license plates and the make/model of vehicles. They are not taking photos of people or property. Chief Hartrum put up a great video explaining the Flock system and how the department is using it if you would like to check that out on the Pentwater PD Facebook page.

I am here to answer any additional questions remotely and can of course still make time to meet with you next week if you would like.

Best Regards,

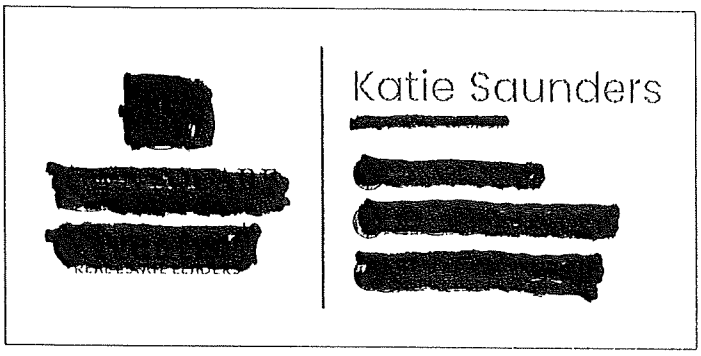
Rachel Witherspoon
Village Manager
Village of Pentwater
(231) 869-8301 Ext. 1

From: Katie Saunders [redacted]
Sent: Tuesday, July 22, 2025 2:17:22 PM
To: Rachel Witherspoon <rwitherspoon@pentwatervillage.org>
Subject: [redacted]

Hi Rachel,

I am not looking to make a fuss but wondering if you could meet me at my house sometime. I have a flock camera pointed right at my house and although we aren't doing anything illegal, it's creepy and I'm sure you'd agree if saw it. I am usually around and it could be quick.. I know you are very busy!

Thanks in advance,
Katie



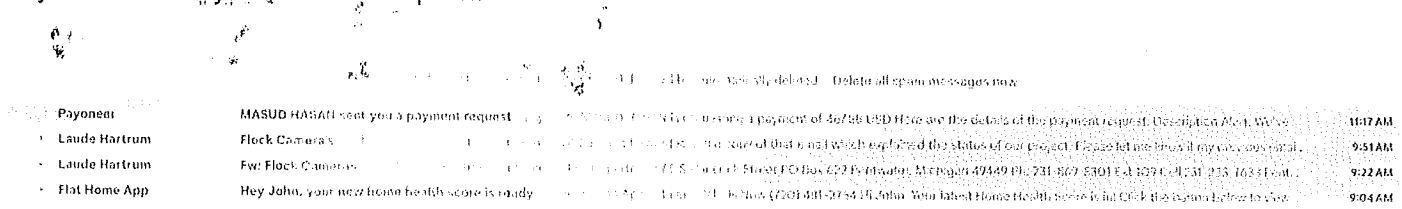
Outlook

Re: Flock Camera's

From John Combs [redacted]
Date Mon 9/14/2026 3:37 PM
To Laude Hartrum <lhartrum@pentwatervillage.org>

Thank you Chief,

Your emails today went to spam so I assume the prior ones did too. I just happened to see them today but normally don't check spam.



I'll be anxious to see your report. I have no doubt that such technology can assist in solving the serious crime issues in Pentwater (if they exist), but my objections are fundamentally to the mass surveillance of law-abiding citizens and loss of Pentwater's data to the nationwide network accessible by thousands of outside agencies. External agencies can query Pentwater and other local towns' travel logs for out-of-state civil matters, immigration enforcement, or reproductive healthcare monitoring—overriding village governance. I am an immigration lawyer and have never seen in my 40 years of this law practice, the extent of lawless detentions and other actions (including murder), by ICE and other federal agencies such as we are seeing these days.

I trust your report will be made available to the public.

Thank you,

John Combs

On Mon, Sep 14, 2026 at 9:51 AM Laude Hartrum <lhartrum@pentwatervillage.org> wrote:

John,

I replied to your last email on 8/24/26. I just forwarded you a copy of that email which explained the status of our project.

Please let me know if my previous emails leave you with any new questions. I can be reached on cell phone or here at the office.

Chief Laude Hartrum
Pentwater Police Department
65 S Hancock Street
PO Box 622
Pentwater, Michigan 49449
Ph. 231-869-8301 Ext 109
Cell 231-233-7633

Outlook

Fw: VILLAGE OF PENTWATER Website: "Report a Concern" Message Alert

From James Van Ess <jvaness@pentwatervillage.org>
Date Mon 9/28/2026 8:11 PM
To Laude Hartrum <lhartrum@pentwatervillage.org>

James "Toby" Van Ess
Village of Pentwater Manager
[redacted]

From: James Van Ess <[redacted]>
Sent: Monday, September 28, 2026 8:11 PM
To: m.wallace2506@gmail.com <m.wallace2506@gmail.com>; Manager <manager@pentwatervillage.org>
Subject: Re: VILLAGE OF PENTWATER Website: "Report a Concern" Message Alert

I will forward this onto the chief and he will include it in his report to council at the October meeting.

James "Toby" Van Ess
Village of Pentwater Manager
231-869-8301 ext. 1

From: pentwater@citywebcentral.com <pentwater@citywebcentral.com>
Sent: Monday, 28 September 2026 20:07:07
To: Manager <manager@pentwatervillage.org>
Subject: VILLAGE OF PENTWATER Website: "Report a Concern" Message Alert

[illegible] Pentwater
[illegible] Concern" Alert

Discover
PENTWATER

Sent by a visitor via the "Report a Concern" form
on the Village of Pentwater website:

Your Name:	Mike Wallace
Street Address:	[redacted]
City, State, Zip:	Pentwater, mi
Telephone:	[redacted]
Email Address:	[redacted]
Message:	I wish to voice my strong opposition to flock cameras within the village.
Submitted On:	2026-09-28 20:07:06
IP Address:	68.43.182.87

Village of Pentwater
65 S. Hancock Street
P.O. Box 622
Pentwater, Michigan 49449

Phone: (231)-869-8301

Outlook

Fw: VILLAGE OF PENTWATER Website: "Report a Concern" Message Alert

From Manager <manager@pentwatervillage.org>
Date Mon 9/28/2026 8:09 PM
To Laude Hartrum <lhartrum@pentwatervillage.org>

Get Outlook for iOS

From: Manager <manager@pentwatervillage.org>
Sent: Monday, September 28, 2026 8:09 PM
To: [redacted]
Subject: Re: VILLAGE OF PENTWATER Website: "Report a Concern" Message Alert

I will forward this onto the Chief. He is compiling his report now and will present at the October council meeting.

Get Outlook for iOS

From: pentwater@citywebcentral.com <pentwater@citywebcentral.com>
Sent: Monday, 28 September 2026 19:57:39
To: Manager <manager@pentwatervillage.org>
Subject: VILLAGE OF PENTWATER Website: "Report a Concern" Message Alert

Pentwater
Concern" Alert

Discover
PENTWATER

Sent by a visitor via the "Report a Concern" form
on the Village of Pentwater website:

Your Name: James Wallace

Organization: [redacted]

Street Address:	[redacted]
City, State, Zip:	Pentwater, Mi. 49449
Telephone:	[redacted]
Email Address:	[redacted]
Message:	I would like to add my name in opposition to "flock cameras". I feel I'm living in a police state whenever I see these obtrusive cameras. If the village council feels we need these cameras do to crime I must be living in an reality. There is no justification for this invasion of my privacy of my travels.The cost also is not justifiable as our tax burden is already high enough.
Submitted On:	2026-09-28 19:57:39
IP Address:	50.36.224.129

Village of Pentwater
65 S. Hancock Street
P.O. Box 622
Pentwater, Michigan 49449

Phone: (231)-869-8301

Outlook

Flock Cameras

From John Combs <[redacted]>
Date Thu 10/1/2026 1:45 PM
To Laude Hartrum <lhartrum@pentwatervillage.org>

2 attachments (4 MB)
Flock Legal Chief Cites Uphill Battle To Ease Lawmakers' Fears.pdf; Leaving-the-Door-Wide-Open-Flock-WA.pdf;

Hello Chief,

As you prepare your report this month, I urge you to review these two attachments.

Even Flock's chief legal officer is worried about what his company's systems could lead to.

As noted in the University of Washington's study, the data is not secure:

- Records obtained by UWCHR researchers via public records requests reveal that at least eight Washington state law enforcement agencies enabled direct, 1:1 sharing of their networks with U.S. Border Patrol at some point during 2025; effectively opening the "front door" for searches potentially related to civil immigration enforcement activities.
- Flock audits reveal apparent "back door" access by U.S. Border Patrol to the networks of at least ten Washington police departments which did not explicitly authorize Border Patrol searches of their network data.
- Flock audits reveal limited cases of law enforcement agencies in Washington state conducting "side door" searches on behalf of federal immigration enforcement agencies, as well as numerous similar searches by other law enforcement agencies nationwide with access to Flock networks in Washington state.
- Discrepancies between Flock audits and other documentation make it impossible for independent researchers to determine the current scope of local organizations' access and exposure to searches by other Flock users nationwide.

Will you please send me a copy of your report when it is complete?

Thank you,
John Combs

On Mon, Sep 14, 2026 at 9:22 AM Laude Hartrum <lhartrum@pentwatervillage.org> wrote:

> Chief Laude Hartrum
> Pentwater Police Department
> 65 S Hancock Street
> PO Box 622

Pentwater, Michigan 49449
Ph. 231-869-8301 Ext 109
Cell 231-233-7633

Pentwater Police Department Confidentiality Notice

This email and any attached documents may contain confidential information, belonging to the sender, which is legally privileged. This information is intended only for the use of the individual or entity named above. The authorized recipient of this information is prohibited from disclosing this information to any other party. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is strictly prohibited. If you have received this email in error, please notify the sender immediately and delete all copies of the email from your system.

From: Laude Hartrum <lhartrum@pentwatervillage.org>
Sent: Monday, August 24, 2026 11:56 AM
To: [redacted]
Cc: James Van Ess <jvaness@pentwatervillage.org>
Subject: Flock Cameras

John,

Thanks for reaching out and asking the question.

Currently, the Pentwater Police Department is engaged in a 90-Demonstration project with Flock Safety. The Project is called Alastor. We have six active cameras in Pentwater. The location of the camera was made on our best guess of traffic patterns.

The cameras take pictures of vehicles and license plates. They are not connected with Secretary of State, NCIC (This is a national database of active arrest warrants), LEIN (Law Enforcement Information System). In order to obtain any information beyond the pictures and the license plate numbers, we are required to have a valid reason and a complaint number (police report).

The purpose of the Project is to determine: First, is the technology reliable and does it provide valid information: Second, to determine how the technology be best be used to meet the goals of the police department: Third, to determine how best to manage and monitor the use of the technology: Finally, to provide the Village of Pentwater, and the Village Council with the best information possible in order to make a decision as we move forward.

Project Alastor was originally coordinated with the Oceana County Sheriff's Office, but the Sheriff's Office decided to suspend their Project after about 14 days. They have issued no report and have made no evaluation.

Due to a rather strange set of circumstances the cameras in Pentwater have been up for over a year, consequently we have quite a lot of experience with them. The Project has not cost the Village of Pentwater any money.

The Project will be concluded on October 28th of this year and at that time I will be submitting an evaluation and my recommendations to the Village Council / Village Manager. Currently, there are no funds allocated to support the camera system. The cost of each camera per year is approximately $3,600. The Council will have to allocate additional funding if they determine that they want to maintain any or all of the cameras.

We have 45 days after the project ends to make a final decision.

If you would like to come in and the software interface and discuss the cameras in more detail, I would be happy to show you how they work and include your opinion in our evaluation.

Chief Laude Hartrum
Pentwater Police Department
65 S Hancock Street
PO Box 622
Pentwater, Michigan 49449
Ph. 231-869-8301 Ext 109
Cell 231-233-7633

Pentwater Police Department Confidentiality Notice

This email and any attached documents may contain confidential information, belonging to the sender, which is legally privileged. This information is intended only for the use of the individual or entity named above. The authorized recipient of this information is prohibited from disclosing this information to any other party. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is strictly prohibited. If you have received this email in error, please notify the sender immediately and delete all copies of the email from your system.

Bloomberg Law

Request a Demo Login

Business & Practice
Exclusive

Flock Legal Chief Cites Uphill Battle To Ease Lawmakers' Fears

Sept. 25, 2026, 3:00 AM MDT

Dan Haley's soon-to-be boss warned him a little over a year ago: Taking the helm of the legal department at Flock Safety — maker of license plate readers facing a growing, national backlash over their potential use for mass surveillance — would come with unique scrutiny.

"The scrutiny came harder and faster than I expected," Haley, now Flock's chief legal officer, said in a recent interview with Bloomberg Law.

Congressional probes. A half-dozen states — including Florida, California, and Texas — either banning the systems or suing Flock users. Cities rupturing their contracts. Lawsuits alleging constitutional violations. Residents destroying Flock cameras. And a Washington hearing this week in which Sen. Josh Hawley(R-Mo.) and other lawmakers threatened legislation and subpoenas against Flock CEO Garrett Langley and executives from competitors who were no-shows at the hearing.

Haley, in an interview two weeks before that hearing, said he's been busy growing his legal department, sharpening ties with Washington, and countering the growing narrative that Flock's cameras are invasive. The company unveiled new privacy safeguards last month, committing to shorten how long information is retained, restrict customers' searches of data, and require audit logs tracking user activity.

Still, some of Flock's efforts to win over policymakers have been "an uphill battle," Haley said.

"People have concerns about government overreach, about government authority, about surveillance, about their data. All of these things are legitimate concerns," Haley said. "It's a fascinating challenge to both navigate the legal questions — which in a very weird way are the easy part of the equation right now — as opposed to the public policy part of the equation, the public perception part of the equation, the public trust part of the equation."

The Poster Child

Flock Safety has become the poster child for automatic license plate readers in the US, which can capture vehicles' make, model, and color, as well as identify people in cars and physical vehicle attributes such as damage or political bumper stickers.

Cities across the country have installed Flock's cameras, which are praised by police departments for helping them rapidly identify vehicles associated with crimes. Flock has deployed more than 120,000 cameras in 49 states and counts at least 5,000 law enforcement agencies and a thousand businesses as customers.

The private company raised a $200 million equity round and $300 million in venture debt at an $8.3 billion valuation earlier this year, Bloomberg reported.

To stimulate the startup's expansion and field legal and regulatory push-back, Haley said he's grown Flock's legal team, bringing on staff with compliance, public policy, and litigation experience.

"It's been easier for me to advocate for resources because the need is self-evident," said Haley, who succeeded Mark Smith after his three-year stint as general counsel. "No CEO wants to add lawyers ever, but I've had a fairly easy time hiring people with good experience, good subject matter expertise in the policy arena, litigation support, and also happily in deal support because our deals get more complex as our product gets more complex."

Eyes on Washington

Haley works out of a home office 30 minutes outside of Boston, when he's not taking trips about once a month to Flock's headquarters in Atlanta. That's until more recently, he said, when he started spending some time in Washington.

Flock spent more than $400,000 on federal lobbying in the first half of 2026, according to disclosure filings. It also recently retained the Republican lobbying firm Off Hill Strategies to help handle Congressional concerns.

Hawley, the senior senator from Missouri, has been among the company's most vocal critics in Washington. He opened an investigation into Flock's data collection, retention, and sharing last month, before broadening his probe a few days later to include Motorola Solutions, Verkada, and Axon Enterprise. CEOs from those three Flock competitors also declined invitations to this week's hearing.

Langley's absence on the Capitol Hill stood out given Flock's campaign this year to defend its practices to concerned residents, lawmakers, and regulators.

Flock said in a statement Thursday that the company has "been working in good faith" to address Hawley's questions, including by "providing a comprehensive response to his inquiry and an in-depth demonstration for Committee staff of Flock's technology and the safeguards governing its use." It didn't directly address why it skipped the hearing.

The startup said it's supported legislation in multiple states and would "welcome the opportunity" to do the same at the federal level.

"One of the absolute best ways to gain credibility with policymakers is just to answer questions, be willing to listen to a question and answer it to the best of your knowledge," Haley said in the earlier interview.

Verkada said its CEO was unable to attend the hearing but that the company has also been engaging with Subcommittee members. Motorola and Axon didn't respond to requests for comment.

Federal lawmakers have introduced bills that would bar federal agencies from purchasing or deploying automated surveillance systems, or withhold funding from cities using such cameras. State officials from Arizona, Florida, Connecticut, California, and Texas, among others, have ended their contracts with the startup, sued cities and police departments using the technology, banned the use of cameras, or opened investigations.

"I understand entirely that some people might look at Flock and say, 'Even if I believe everything you're saying about your technology and the safeguards and everything else, your technology could someday be the infrastructure for a surveillance state, and that makes me worried,'" Haley said. "And my response to that is, 'Me too.'"

— With assistance from Caitlin Oprysko.

To contact the reporter on this story: Cassandre Coyer in Washington at ccoyer@bloombergindustry.com

To contact the editors responsible for this story: Jeff Harrington at jharrington@bloombergindustry.com; Adrianna Rodriguez at arodriguez1@bloombergindustry.com

© 2026 Bloomberg Industry Group, Inc. All Rights Reserved



LEAVING THE DOOR WIDE OPEN

FLOCK SURVEILLANCE SYSTEMS EXPOSE WA DATA TO IMMIGRATION ENFORCEMENT

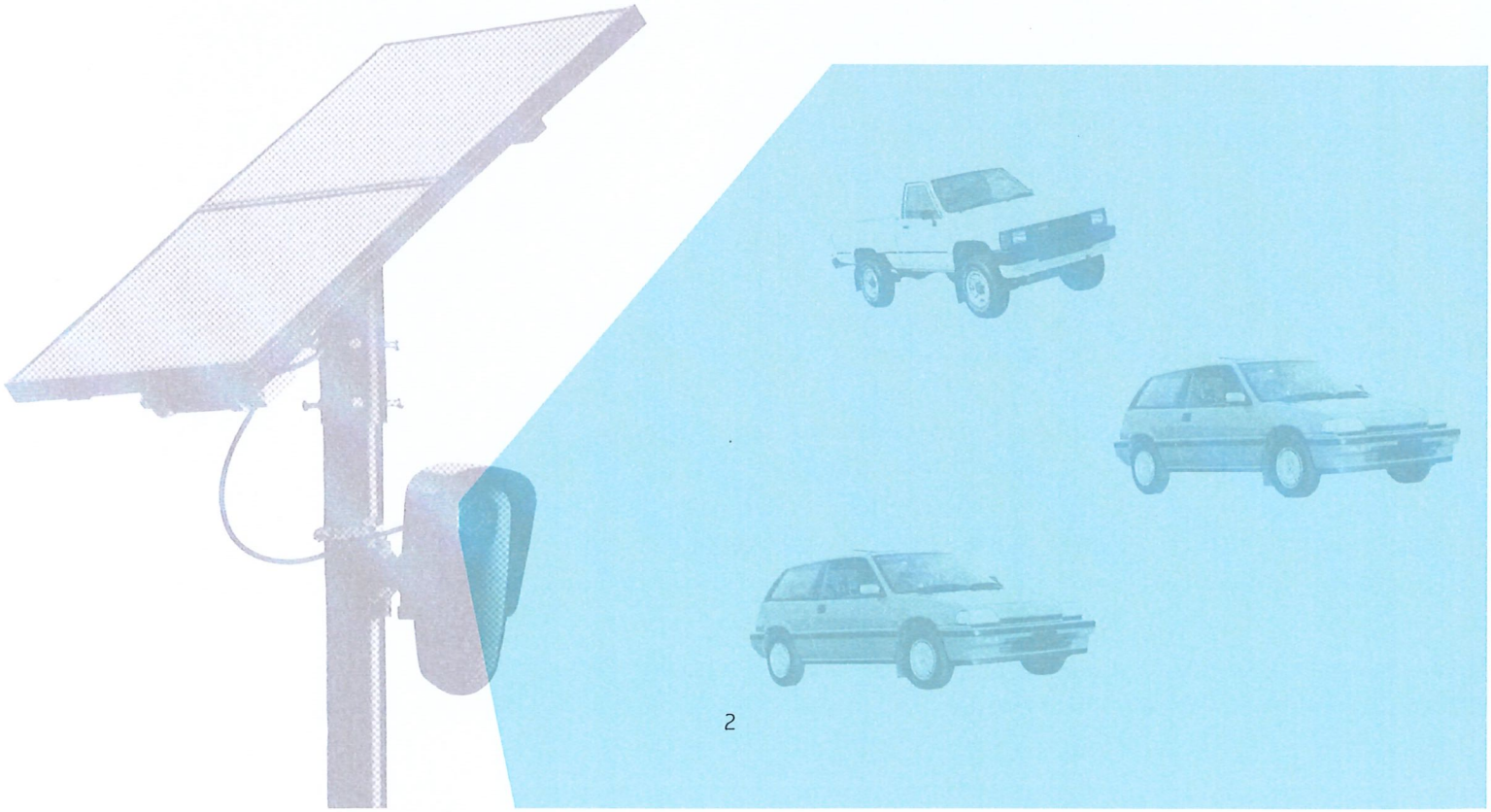
UNIVERSITY *of* WASHINGTON
CENTER FOR HUMAN RIGHTS
HENRY M. JACKSON SCHOOL OF INTERNATIONAL STUDIES

Leaving the Door Wide Open:
Flock Surveillance Systems Expose Washington Data to Immigration Enforcement

University of Washington
October 2025

The University of Washington Center for Human Rights is committed to interdisciplinary excellence in the education of undergraduate and graduate students in the field of human rights; promoting human rights as a core area of faculty and graduate research; and engaging productively with local, regional, national, and international organizations and policymakers to advance respect for human rights.

Center for Human Rights
The Henry M. Jackson School of International Studies
University of Washington
Box 353650, Seattle, WA 98195-3650
Phone: (206) 685-3435 | Email: uwchr@uw.edu
www.jsis.washington.edu/humanrights



CONTENTS

Summary 4

Introduction 4

Background 7

Research Methodology 11

Findings 12

- *"Front door" access* 13
- *"Back door" access by Border Patrol to Flock Networks* 14
- *"Side door" searches on behalf of federal immigration enforcement agencies* 16
- *Discrepancy between Flock audits and access settings* 19

Conclusions 20

Appendix 22

SUMMARY

- Flock Safety automated license plate reader (ALPR) networks have become increasingly common in Washington state.
- Records obtained by UWCHR researchers via public records requests reveal that at least eight Washington state law enforcement agencies enabled direct, 1:1 sharing of their networks with U.S. Border Patrol at some point during 2025; effectively opening the "front door" for searches potentially related to civil immigration enforcement activities.
- Flock audits reveal apparent "back door" access by U.S. Border Patrol to the networks of at least ten Washington police departments which did not explicitly authorize Border Patrol searches of their network data.
- Flock audits reveal limited cases of law enforcement agencies in Washington state conducting "side door" searches on behalf of federal immigration enforcement agencies, as well as numerous similar searches by other law enforcement agencies nationwide with access to Flock networks in Washington state.
- Discrepancies between Flock audits and other documentation make it impossible for independent researchers to determine the current scope of local organizations' access and exposure to searches by other Flock users nationwide.

INTRODUCTION

In recent months, amidst a national campaign of mass deportation, concerns have spread among Washington state residents about local and state authorities' improper sharing of their personal data with federal government agencies involved in immigration enforcement. Some of these concerns revolve around license plate data, which UWCHR researchers have found are frequently cited in Immigration and Customs Enforcement (ICE) records as a tool used in the identification and location of targets. In July, a reporter from King 5 News discovered that Immigration and Customs Enforcement and other federal agencies had made thousands of searches of the Driver and Plate Search (DAPS) database from Washington state's Department of Licensing (DOL), resulting in immigration arrests.[1] While the DOL has said that it has now suspended fourteen federal agencies' access to the DOL's DAPS database,[2] surveillance technology such as automated license plate readers (ALPRs) offer another source of information about Washington drivers. And in recent months, UWCHR researchers have learned that ALPR data collected by local law enforcement agencies across our state is being frequently accessed by federal agencies involved in immigration enforcement, despite the protections embedded in Washington's Keep Washington Working law.

1 Kristin Goodwillie, "Washington state agency under fire for sharing drivers' data with ICE," *King 5*, July 21, 2025, https://www.king5.com/article/news/investigations/investigators/washington-state-license-agency-under-fire-for-sharing-drivers-data-with-ice/281-c38e5569-b500-4f19-9a2c-660af-77a4fc9

2 In a September 19, 2025 meeting with community advocates, the DOL's Alejandro Sánchez said that 14 federal agency accounts had been suspended due to their failures to submit materials certifying that they had complied with the database's permissible use standards. It is important to note that these accounts have been suspended, rather than terminated; it is unclear, should agencies now assert they are in compliance, whether they would be reinstituted on the basis of those assertions.

In December 2022, UWCHR published a report, "Who's Watching Washington?", which discussed rights concerns raised by ALPRs and related technologies, including their potential uses for immigration enforcement and the criminalization of reproductive healthcare access. While DOL's DAPS database makes it possible to identify a vehicle's registered owner by searching a full or partial license plate number,[3] ALPRs make it possible to pinpoint that vehicle's location as it moves through the world; they even enable automatic notifications when a vehicle included on a "hot list" drives by a device in the user's network. They may be a potent tool for law enforcement,[4] but as UWCHR warned in 2022, their misuse can undermine the reproductive and migrant rights which Washington state has committed itself to defending.[5]

Since that time, usage of ALPRs by local governments and private parties alike has continued to expand, and one company, Flock Safety, has come to dominate the market. While there is no comprehensive data on the proliferation of Flock Safety systems, a recent report by The Urbanist suggests that the systems are used by at least 80 cities, six counties, and three Tribal governments in Washington state.[6] Agencies employing these systems include local police and sheriffs, school districts, public housing authorities, and more;[7] in addition to public entities, private businesses and neighborhood associations are part of the Flock network, often sharing images captured by their devices with law enforcement.

---

3 DAPS also permits address searches, which allow the user to obtain data about all residents of a given address who have drivers licenses.

4 Their actual effectiveness at helping solve or prevent crimes is disputed, however. See Jonathan Hofer, *Efficacy of Automated License Plate Reader Hits in Piedmont, California*, Secure Justice and Independent Institute, August 3, 2022, https://static1.squarespace.com/static/5edeeebc3032af28b09b6644/t/64a46a417c2a6637212e1ce3/1688496710563/2021_11_30_alpr.pdf; Gowri Saini Balasubramaniam, Clara Belitz, and Anita Say Chan, "Bridging Informational Divides: A Community-Centered Analysis of 'Public Safety' Surveillance Technology," *Association for Computing Machinery*, May 2024, https://dl.acm.org/doi/10.1145/3613905.3644046; and John Shjarback and James Sarkos, J. A, "An Evaluation of a Major Expansion in Automated License Plate Reader (ALPR) Technology," *Justice Evaluation Journal*, March 6, 2025, https://doi.org/10.1080/24751979.2025.2473363. On the other hand, representatives of Flock offer their own analysis which finds the systems to be very effective: see Adam Snow et al, "Flock Safety Technologies in Law Enforcement: An Initial Evaluation of Effectiveness in Aiding Police in Real-World Crime Clearance," *Research Gate*, January 2024, https://www.researchgate.net/profile/Johnny-Nhan/publication/377845222_Flock_Safety_Technologies_in_Law_Enforcement_An_Initial_Evaluation_of_Effectiveness_in_Aiding_Police_in_Real-World_Crime_Clearance/links/65c1020d7900745497673897/Flock-Safety-Technologies-in-Law-Enforcement-An-Initial-Evaluation-of-Effectiveness-in-Aiding-Police-in-Real-World-Crime-Clearance.pdf

5 On Washington state protections for reproductive rights, Washington law recognizes protection for abortion as a fundamental right (see Wash. Rev. Code § 9.02.100 (1992), https://app.leg.wa.gov/rcw/default.aspx?cite=9.02.100); other, more recent legislation has instituted further protections, including Washington's Shield Law (HB 1469), passed in 2023, which protects those providing or seeking reproductive and gender-affirming healthcare from civil or criminal actions in other states (see Washington State Office of the Attorney General, "Reproductive and Gender-Affirming Care: Shielding Providers, Seekers, and Helpers From Out-of-State Legal Actions", https://www.atg.wa.gov/reproductive-and-gender-affirming-care-shielding-providers-seekers-and-helpers-out-state-legal); and additional measures described here: Jerry Cornfield, "Washington's bold new abortion protections in spotlight at White House," *Washington State Standard*, June 15, 2025, https://washingtonstatestandard.com/2023/06/15/washingtons-bold-new-abortion-protections-in-spotlight-at-white-house/. On the matter of immigrant rights, the Keep Washington Working Act (2020), implemented in Wash. Rev. Code § 10.93.160, https://app.leg.wa.gov/RCW/default.aspx?cite=10.93.160, is the best known of a series of laws passed in recent years to ensure Washington remains welcoming to migrants, though recent years have seen the passage of multiple other laws to strengthen this commitment; see Jacquelyn Jimenez Romero, "Trio of immigrant rights laws signed by WA governor," *Washington State Standard*, May 14, 2025, https://washingtonstatestandard.com/2025/05/14/trio-of-immigrant-rights-laws-signed-by-wa-governor/.

6 Amy Sundberg, "License Plate Readers Proliferate in Washington, Bringing Concerns over ICE Overreach," *The Urbanist*, June 19, 2025, https://www.theurbanist.org/2025/06/19/license-plate-readers-proliferate-in-washington-ice-overreach/

7 EFF's Atlas of Surveillance lists 75 Washington state agencies with Flock contracts https://www.atlasofsurveillance.org/; DeFlock, an organizing initiative that opposes the use of the technology, has published a map of the locations and characteristics of 776 ALPR devices (not all of which are Flock Safety devices) in Washington state, see https://deflock.me/map#map=12/47.306241/-121.956825.

Both locally[8] and nationwide,[9] the rapid expansion of Flock ALPRs has generated controversy; many have expressed concerns related to privacy impacts and the systems' possible use for civil immigration enforcement and/or to criminalize access to reproductive healthcare. Similarly, ALPR data is among the forms of surveillance that could be used to criminalize those seeking gender affirming healthcare, as privacy advocates have warned.[10]

Based on analysis of records received from 31 of the law enforcement agencies in Washington state known to be Flock customers,[11] as well as our review of patterns emerging from Flock use in other states, UWCHR researchers conclude that these concerns about Flock Safety systems are well founded. Specifically, our research shows that, in Washington state in 2025:

- At least eight local law enforcement agencies appear to have enabled 1:1 sharing of their Flock Network with Border Patrol at some point during 2025, including Benton County Sheriff's Office and police departments in the cities of Arlington, Auburn, Lakewood, Richland, Sunnyside, Wenatchee, and Yakima.
- The Border Patrol had apparent "back door" access to license plate data captured by ALPRs operated by at least ten local law enforcement agencies across our state which had not explicitly authorized sharing with Border Patrol, from at least May to August 2025.
- In a limited number of cases, local law enforcement agencies in Washington state conducted searches of Flock ALPR data on behalf of Immigration and Customs Enforcement (ICE) or Border Patrol. In addition, law enforcement agencies outside of Washington state conducted numerous "side door" searches of Washington data gathered by Flock networks in our state.
- Serious questions remain about the transparency and accuracy of Flock's descriptions of its own technology, and about users' ability to control and understand its potential impacts.

WHILE DOL'S DAPS DATABASE MAKES IT POSSIBLE TO IDENTIFY A VEHICLE'S REGISTERED OWNER BY SEARCHING A FULL OR PARTIAL LICENSE PLATE NUMBER, ALPRS MAKE IT POSSIBLE TO PINPOINT THAT VEHICLE'S LOCATION AS IT MOVES THROUGH THE WORLD.

8 On the expansion of surveillance technology including Flock Safety in Washington state, see Brandon Block, "Federal aid is supercharging local WA police surveillance tech," *Investigate West*, July 26, 2023, https://www.investigatewest.org/federal-aid-is-supercharging-local-wa-police-surveillance-tech/
The introduction of such technology has been met with opposition in localities including Mountlake Terrace (see Mountlake Terrace: Taylor Scott Richmond, "Mountlake Terrace public express ongoing ire with future Flock system," Everett Daily Herald, August 9, 2025, https://www.heraldnet.com/news/mountlake-terrace-public-express-ongoing-ire-with-future-flock-system/); and was put on hold by the City of Stanwood due to questions about whether Flock video feeds constitute public records: Jenna Peterson, "Stanwood pauses Flock cameras amid public records lawsuits," *Everett Daily Herald*, September 10, 2025, https://www.heraldnet.com/news/stanwood-pauses-flock-cameras-amid-public-records-lawsuits/

9 For reporting on concerns regarding the technology in Virginia, see Kunle Falayi, "The feds' hidden immigration weapon: Virginia's surveillance network," *VPM News*, July 7, 2025, https://www.vpm.org/news/2025-07-07/vcij-immigration-enforcement-flock-safety-license-plate-readers-poggen-klass; in the city of Evanston, Illinois, local officials covered Flock cameras after cancelling a contract with the company: Richard Requena, "After Evanston fires Flock, it reinstalls license-plate readers, so Evanston covers them," *Chicago Tribune*, September 30, 2025, https://www.chicagotribune.com/2025/09/29/after-evanston-fires-flock-it-reinstalls-license-plate-reader-so-evanston-covers-them/

10 René Kladzyk, *Policing Gender: How Surveillance Tech Aids Enforcement of Anti-Trans Laws*, Project on Government Oversight, June 28, 2023, https://www.pogo.org/investigations/policing-gender-how-surveillance-tech-aids-enforcement-of-anti-trans-laws

11 For an overview of agencies whose records were reviewed by UWCHR researchers, see the Appendix to this report.

BACKGROUND

Founded as a startup in 2017, Flock Safety has expanded rapidly by offering low-cost, solar-powered cameras that connect wirelessly to a nationwide network;[12] Forbes has described the company's growth as "explosive."[13] Today, Flock reportedly has more ALPRs in service across the country than any of its competitors.[14] The company boasts more than 80,000 AI-powered cameras across 49 U.S. states, and it is now rolling out a complementary new product: surveillance drones.[15]

Flock ALPRs capture images of all cars that pass the camera; those images are then read by AI, generating text which is stored in Flock's centralized database. Via Flock's user interface, users are able to tap into this database to perform searches—by license plate number, color and make of car, or even details about the car's physical condition such as bumper stickers, a roof rack, or a broken window.[16] The software also reportedly contains features giving users the ability to analyze patterns of movement, to flag repeat visitors to a given area, project information onto maps, analyze vehicles frequently seen in proximity to one another, and generate lists of vehicles that have visited specific locations of interest.[17]

According to Flock, the breadth of data to which a given user has access when doing a search depends on the settings inputted by other users of the system. Each organization that connects to the system has its own network (defined as its own cameras and software), and can choose whether to share the data generated by that network with other law enforcement agencies located in the same state, located within a given geographic radius, or nationwide. It can also identify specific law enforcement agencies with which it chooses to share its data. It could also choose to not share data outside its own network at all.[18]

Besides law enforcement, many businesses, neighborhood associations, and other groups also use Flock. These private customers can opt to have the data generated by their cameras automatically shared with law enforcement, and many do—including major retailers like Home Depot and Lowe's,[19] or Simon Properties, the nation's largest network of shopping malls[20]—but according to Flock, private customers are not able to search data generated by law enforcement ALPRs. (Significantly, unlike all its major competitors in the ALPR market, Flock has refused to allow independent security analysts to test its devices to ensure that claims made by the company are accurate.[21]) Although

12 Jay Stanley, *Fast-Growing Company Flock is Building a New AI- Driven Mass-Surveillance System*, ACLU, March 3, 2022, https://www.aclu.org/report/fast-growing-company-flock-building-new-ai-driven-mass-surveillance-system.

13 Thomas Brewster, "AI Startup Flock Thinks It Can Eliminate All Crime In America," *Forbes*, September 3, 2025, https://www.forbes.com/sites/thomasbrewster/2025/09/03/ai-startup-flock-thinks-it-can-eliminate-all-crime-in-america/

14 Falayi, "The feds' hidden immigration weapon: Virginia's surveillance network."

15 Brewster, "AI Startup Flock Thinks It Can Eliminate All Crime In America," and James O'Donnell, "Shoplifters could soon be chased down by drones," *MIT Technology Review*, September 25, 2025, https://www.technologyreview.com/2025/09/25/1124088/shoplifters-could-soon-be-chased-down-by-drones/.

16 Joseph Cox, "Inside 'TALON,' the Nationwide Network of AI-Enabled Surveillance Cameras," *Vice*, March 3, 2021, https://www.vice.com/en/article/bvx4bq/talon-flock-safety-cameras-police-license-plate-reader see also Brewster, "AI Startup Flock Thinks It Can Eliminate All Crime In America."

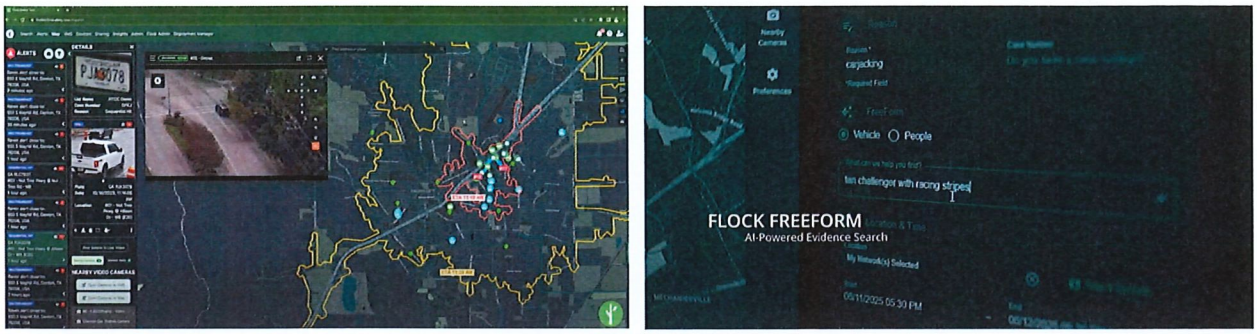
17 Lee Schmidt and Crystal Arrington v. City of Norfolk, Norfolk Police Department, and Mark Talbot, 2:24-cv-621, p. 8, (U.S. District Court for the Eastern District of Virginia Norfolk Division, 2024), http://ij.org/wp-content/uploads/2024/10/2024.10.21-1-Complaint.pdf.

18 Flock Safety, "Setting the Record Straight: Statement on Flock Network Sharing, Use Cases, and Federal Cooperation," June 19, 2025, https://www.flocksafety.com/blog/statement-network-sharing-use-cases-federal-cooperation

19 Jason Koebler, "Home Depot and Lowe's Share Data From Hundreds of AI Cameras With Cops," *404 Media*, August 6, 2025, https://www.404media.co/home-depot-and-lowes-share-data-from-hundreds-of-ai-cameras-with-cops/

20 Thomas Brewster, "America's Biggest Mall Owner Is Sharing AI Surveillance Feeds Directly With Cops," *Forbes*, May 6, 2024, https://www.forbes.com/sites/thomasbrewster/2024/05/06/simon-property-and-flock-safety-feed-ai-surveillance-feeds-to-the-cops/

21 Jay Stanley, "Communities Should Reject Surveillance Products Whose Makers Won't Allow Them to be Inde-



Screenshots from Flock Safety promotional videos reviewing features of Flock tools including phone, plate, or address lookup across systems and jurisdictions, public and private network sharing, AI-powered search and alert systems, geospatial mapping, and more.

concern about the use of Flock's products[22] for immigration enforcement is not new, it spiked following 404 Media's revelations in May 2025 that local police around the country were performing searches of Flock's database on behalf of Immigration and Customs Enforcement (ICE).[23] These "side door" searches were performed by authorized law enforcement users on behalf of ICE, and were only discovered because the person performing the search had typed "ICE," "illegal immigration," or other similar descriptors in the required field where users must input the reason for their search. Of course, in some jurisdictions, local law enforcement collaboration with ICE is perfectly legal; in others, such as Washington, the practice of conducting a search to assist ICE in civil immigration enforcement would run afoul of state law. And what happens when a law enforcement agency in a state that collaborates with ICE gives federal immigration agents access to data, obtained through Flock's network, which was generated by law enforcement ALPRs from a state that bans such collaboration?

Also in May, 404 Media also revealed that a police officer in Texas had conducted nationwide searches of Flock's networks in an effort to track down a woman who had self-administered an abortion; in October 2025, further reporting showed that law enforcement had considered bringing criminal charges against her.[24] Among the data searched was that generated by Flock ALPR networks in Yakima and Prosser, Washington.[25] Reproductive rights advocates expressed alarm that law enforcement in a state where almost all abortions are illegal was using data generated by publicly-operated ALPR systems in Washington, a state committed to ensuring access to abortions for all who need them.[26]

In response to this controversy, Flock's founder and CEO issued a statement in June 2025 in which he emphasized that decisions about with whom to share data, and how they might use it, were up to users themselves: "It is a local decision.

---

pendently Evaluated," *ACLU*, March 6, 2024, https://www.aclu.org/news/privacy-technology/communities-should-reject-surveillance-products-whose-makers-wont-allow-them-to-be-independently-evaluated

22 Flock Safety, "The Future of Policing: A Real-Time Crime Center Playbook," Youtube, August 12, 2025, https://www.youtube.com/watch?v=QcB7IIz4jYA; and Flock Safety, "Real-Time Policing in Action with Flock Safety," Youtube, August 12, 2025, https://www.youtube.com/watch?v=TfeT83cffWA.

23 Jason Koebler and Joseph Cox, "ICE Taps into Nationwide AI-Enabled Camera Network, Data Shows," *404 Media*, May 27, 2025, https://www.404media.co/ice-taps-into-nationwide-ai-enabled-camera-network-data-shows/

24 Jason Koebler and Joseph Cox, "Police Said They Surveilled Woman Who Had an Abortion for Her 'Safety.' Court Records Show They Considered Charging Her With a Crime," *404 Media*, October 7, 2025, https://www.404media.co/police-said-they-surveilled-woman-who-had-an-abortion-for-her-safety-court-records-show-they-considered-charging-her-with-a-crime/?ref=daily-stories-newsletter

25 Jason Koebler and Joseph Cox, "A Texas Cop Searched License Plate Cameras Nationwide for a Woman Who Got an Abortion," *404 Media*, May 29, 2025, https://www.404media.co/a-texas-cop-searched-license-plate-cameras-nationwide-for-a-woman-who-got-an-abortion/

26 "Muckrock user Rose Terse obtained two of the sets of data from Yakima and Prosser police departments in Washington via public records requests": Koebler and Cox, "A Texas Cop Searched License Plate Cameras Nationwide for a Woman Who Got an Abortion."

Name	Org Name	Total Networks S	Total Devices Se	Time Frame	License Plate	Case #	Filters	Reason	Search Time
J. Sha	Stone County MS SO	6293	81326	4/5/2025, 04:38: 5/5/2025, 04:38:		24-09585	Mississippi	CSAM	5/5/2025, 04:39:09 PM UTC
C. New	Wichita KS PD	6499	82720	4/9/2025, 06:49: 5/9/2025, 06:49:				NNC 24-15	5/9/2025, 06:49:07 PM UTC
N. Bla	Boone County IN SO	6325	81888	4/9/2025, 06:49: 5/9/2025, 06:49:			Indiana	warrant	5/9/2025, 06:49:07 PM UTC
M. Har	Greenville County SC SO	6009	78275	4/9/2025, 06:49: 5/9/2025, 06:49:			South_carolina	warrant	5/9/2025, 06:49:12 PM UTC
J. Smi	Johnson County TX SO	6809	83345	4/9/2025, 06:48: 5/9/2025, 06:48:		2500002320	Land_rover Texa	had an abortion, search for female	5/9/2025, 06:49:15 PM UTC
J. Ash	Southfield MI PD	6465	82535	4/9/2025, 06:49: 5/9/2025, 06:49:			Michigan	INV	5/9/2025, 06:49:16 PM UTC
C. Nee	Richland County OH SO	6299	81238	4/2/2025, 02:28: 5/2/2025, 02:28:			Ohio	unauthorized	5/2/2025, 02:28:45 PM UTC
A. Hin	Arlington TX PD	5757	76298	4/2/2025, 02:28: 5/2/2025, 02:28:			Texas	stolen	5/2/2025, 02:28:45 PM UTC
G. vog	Lafourche Parish LA SO	6280	80974	4/25/2025, 02:28 5/2/2025, 02:28:			Louisiana	CRIMINAL	5/2/2025, 02:28:58 PM UTC
Z. K	Fayette County GA SO	5774	76603	4/2/2025, 12:52: 5/2/2025, 12:52:				locate	5/2/2025, 12:52:57 PM UTC

An excerpt from a Flock Network Audit from Prosser Police Department shows a May 9, 2025 search of the department's network by a user from the Johnson County Texas Sheriff Office, listing the reason for search as "had an abortion, search for female."

Not my decision, and not Flock's decision."[27] He emphasized the importance of using audits to ensure that users are aware of the data-sharing choices they have enabled on their network. Flock provides customers with two monthly audits: an Organization Audit which reports searches by users internal to the organization of both the local network and any networks shared with it; and a Network Audit, which reports searches of the organization's network by external users. Both of these reports include the same fields of information,[28] including the identity of the user making the search, the organization to which they belong, the date and timeframe of the search, the number of networks and devices searched, the specific license plate number (or partial number) searched for, the "reason" asserted for the search, associated case number, and search filters such as vehicle make or state. The audits only report the contents of each search, not its results; and local agencies make their own determinations about how long to retain the results of searches. In addition, Flock allows users to generate a Network Sharing report which lists networks shared by and with the organization on a 1:1 basis; and maintains Transparency Portals, through which organizations can choose to publicly report various characteristics of their network, including its sharing settings and a limited public audit.

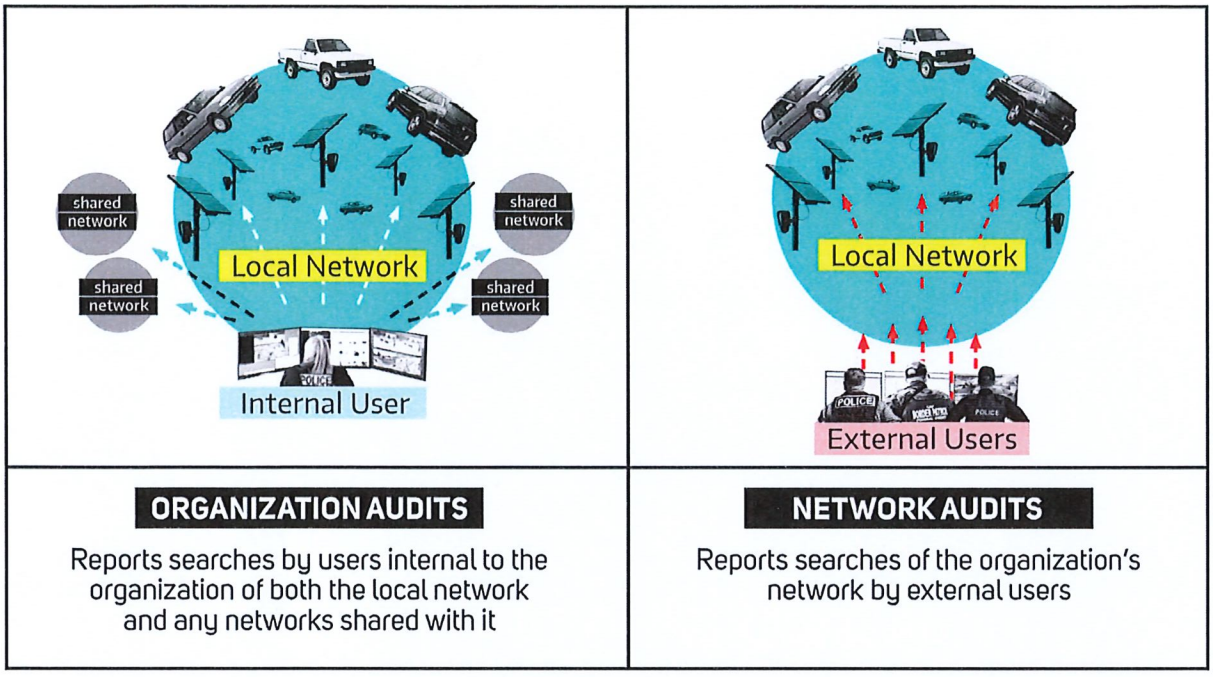
> **REPRODUCTIVE RIGHTS ADVOCATES EXPRESSED ALARM THAT LAW ENFORCEMENT IN A STATE WHERE ALMOST ALL ABORTIONS ARE ILLEGAL WAS USING DATA GENERATED BY PUBLICLY-OPERATED ALPR SYSTEMS IN WASHINGTON, A STATE COMMITTED TO ENSURING ACCESS TO ABORTIONS FOR ALL WHO NEED THEM.**

In August 2025, however, a local news outlet in Colorado discovered that Customs and Border Protection (CBP) had accessed ALPR data in Flock's database generated by customers who had not intended to share with federal authorities.[29] Flock responded that this had occurred through a previously-undisclosed "pilot program," suggesting that despite not having a Flock contract, CBP had sent requests

27 Flock Safety, "Setting the Record Straight: Statement on Flock Network Sharing, Use Cases, and Federal Cooperation."

28 Flock audits released to UWCHR vary due to local jurisdictions' decisions regarding public disclosure; for example, some agencies withheld the "License plate" field, while others released it without redactions.

29 Spencer Soicher, "Flock admits federal immigration agents have direct access to tracking data, despite previous claims," *9News*, August 19, 2025, https://www.9news.com/article/news/local/flock-federal-immigration-agents-access-tracking-data/73-a8aee742-56d4-4a57-b5bb-0373286dfef8?ref=404media.co



Flock users can access various forms of audits and reports, including Organization Audits, which report searches by users internal to the organization of both the local network and any networks shared with it; and Network Audits, which report searches of the organization's network by external users.

for 1:1 data sharing to multiple jurisdictions and many had accepted, implying the practice had been limited.[30] Yet 404 Media notes, "functionally, there is no difference between Flock's 'nationwide network' and the network of cameras that CBP has access to,"[31] suggesting instead that CBP had effectively been granted "back door" access to the entire system. This included data from police departments in Washington state. As 404 Media reported, "Data obtained in separate requests from the Prosser Police Department and Chehalis Police Department, both in Washington state, also show CBP searching a huge number of networks and devices."[32]

Flock responded by acknowledging it had "communicated poorly" and "inadvertently provided inaccurate information," and stressing that it would now designate all federal users as part of a separate "Federal" category in order to make it easier for users to distinguish them, and would not include them in "statewide" or "nationwide" lookup categories.[33] However, privacy watchdogs at the Electronic Frontier Foundation criticized such measures as ineffective, noting that "The possibility of human workarounds at every level undermines any technical safeguards Flock may claim."[34] Specifically, the reliance on user-inputted "reasons" for a search as a means to determine its legitimacy is inherently problematic, especially when users frequently input cryptic abbreviations or vague terms like "investigation" into that field.

30 Ibid.
31 Jason Koebler, "CBP Had Access to More than 80,000 Flock AI Cameras Nationwide," *404 Media*, August 25, 2025, https://www.404media.co/cbp-had-access-to-more-than-80-000-flock-ai-cameras-nationwide/
32 Ibid.
33 Garret Langley, "Ensuring Local Compliance," *Flock Safety*, August 25, 2025, https://www.flocksafety.com/blog/ensuring-local-compliance
34 Sarah Hamid and Rindala Alajaji, "Flock Safety's Feature Updates Cannot Make Automated License Plate Readers Safe," *Electronic Frontier Foundation*, June 27, 2025, https://www.eff.org/deeplinks/2025/06/flock-safetys-feature-updates-cannot-make-automated-license-plate-readers-safe

The growing controversy around Flock prompted a growing number of law enforcement jurisdictions to cancel or suspend their contracts with the company in recent months, including Austin, TX,[35] Syracuse, NY,[36] Berkeley, CA,[37] Scarsdale, NY,[38] Evanston, IL,[39] Oak Park, IL,[40] and Sedona, AZ.[41]

> **THE RELIANCE ON USER-INPUTTED "REASONS" FOR A SEARCH AS A MEANS TO DETERMINE ITS LEGITIMACY IS INHERENTLY PROBLEMATIC, ESPECIALLY WHEN USERS FREQUENTLY INPUT CRYPTIC ABBREVIATIONS OR VAGUE TERMS LIKE "INVESTIGATION" INTO THAT FIELD.**

35 Ben Thompson, "Austin to halt police license plate reader program after public pushback," *Community Impact*, June 19, 2025, https://communityimpact.com/austin/south-central-austin/government/2025/06/04/austin-to-halt-police-license-plate-reader-program-after-public-pushback/

36 Patrick McCarthy, "Syracuse police 'inadvertently' exposed driver data to thousands of cops around the country," *Central Current*, July 4, 2025, https://centralcurrent.org/syracuse-police-exposed-driver-data-to-thousands-of-cops-around-the-country/

37 Eric Urbach, "Berkeley street camera company pauses pilot program amid data sharing concerns," *The Daily Californian*, August 28, 2025, https://www.dailycal.org/news/city/berkeley-street-camera-company-pauses-pilot-program-amid-data-sharing-concerns/article_4853fd4f-1fe7-40da-ba48-9b917f2ebcae.html

38 Justin Arest, *Mayoral Community Update*, Scarsdale, New York, August 6, 2025, https://www.scarsdale.gov/DocumentCenter/View/10994/08062025-Mayoral-Letter?fbclid=IwY2xjawMASBBleHRuA2FlbQIxMABicmlkETE0QU42TGE5RWU1aFlobVNsAR7TX5hjkO2ED7u5Otun9dJybJn0AsdkTaiDiSzxj2WRky1tn-7sTbMl4vPtVw_aem_gH4S6HKpq8AR-bljDxJhGA

39 Bill Smith, "Evanston cancels Flock camera contract," *Evanston Now*, August 27, 2025, https://evanstonnow.com/evanston-cancels-flock-camera-contract/

40 Liz Nagy et al, "License plate reader company under investigation in Illinois speaks out as suburbs end contracts," *ABC7 Chicago*, August 28, 2025, https://abc7chicago.com/post/evanston-oak-park-end-contracts-flock-safety-license-plate-reader-company-investigation-illinois/17678137/

41 Joseph K Giddens, "Sedona City Council tells staff to get Flock out of town," *Sedona Red Rock News*, September 10, 2025, https://www.redrocknews.com/2025/09/10/sedona-city-council-tells-staff-to-get-the-flock-out-of-town/

RESEARCH METHODOLOGY

In July 2025, UWCHR set out to investigate the human rights implications of Flock ALPR use in our state today. Researchers filed public records requests with 48 law enforcement agencies in Washington known to use Flock systems. To date, we have received and reviewed records pursuant to these requests from 35 jurisdictions. We have also reviewed public records requests filed by other researchers using open portals;[42] local and national reporting on Flock systems; and Flock documentation, promotional, and public relations materials.

From each jurisdiction, UWCHR researchers requested copies of Flock Organizational Audits, Network Audits, and Network Sharing settings. In several cases, local public records officers expressed that such records had not previously been requested and appeared not to understand how to access Flock audits or Network Sharing reports. In others, agencies denied UWCHR's public records requests. The city of Sedro-Wooley denied requests for both Flock Organizational Audits and Network Audits, stating: "We have not run reports for either an organization audit or a network audit in Flock, therefore no records exist."[43] Similarly, the cities of Arlington, Everett, Kent, Medina, and Tukwila denied UWCHR's requests for disclosure of Flock Network Audits, arguing that the reports had not been reviewed by their agencies and do not constitute public records. UWCHR is in the process of appealing these determinations.[44]

42 UWCHR researchers are grateful for the following public records requests filed by Rose Terse and made public via Muckrock: Prosser PD, Medina PD, Tukwila PD, Yakima PD (published on May 14, 2025); and Ellensburg PD, Centralia PD (published on May 22, 2025). UWCHR's public records requests were modeled after those filed by Terse in order to permit direct comparison across agencies.

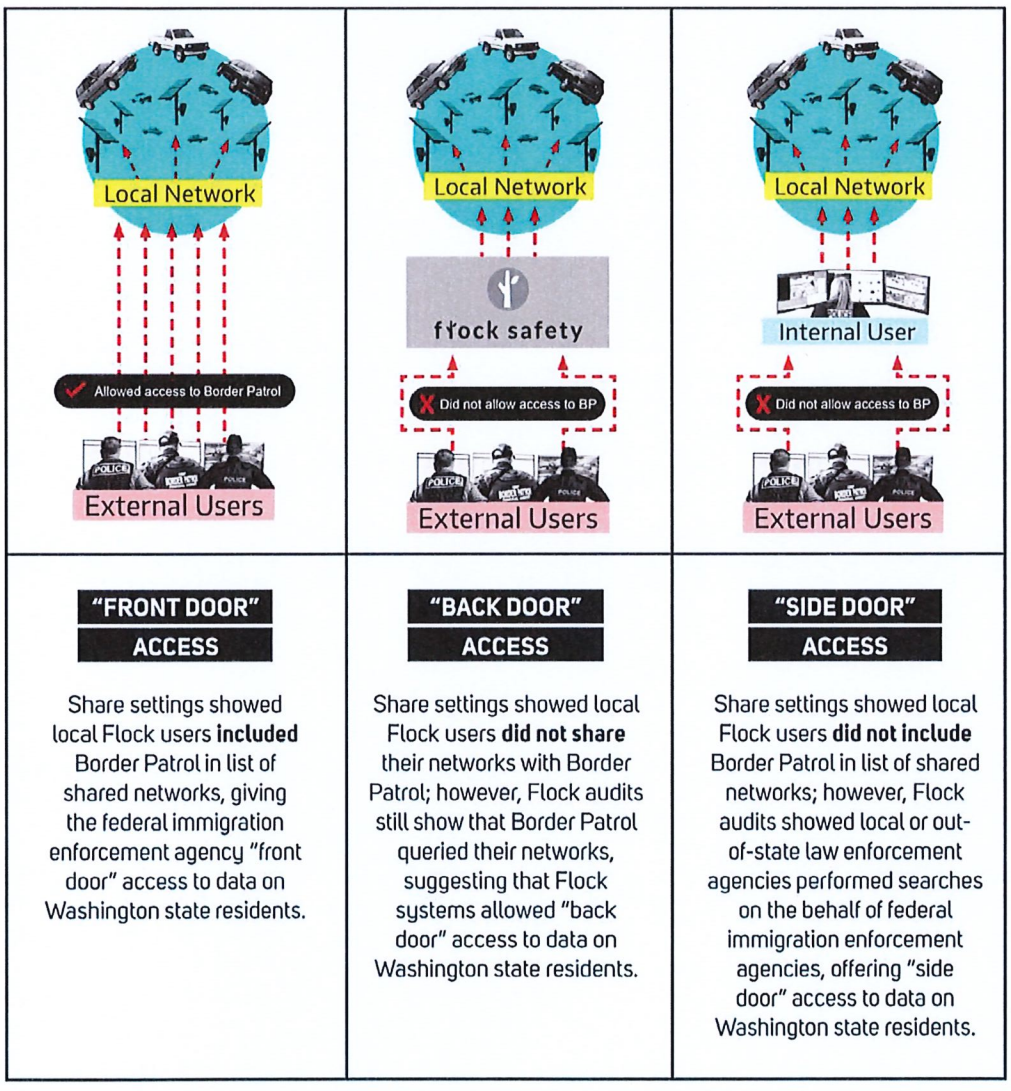
43 UWCHR correspondence with Sedro-Wooley public records officer, Sept. 8, 2025.

44 On August 26, 2025, UWCHR received correspondence

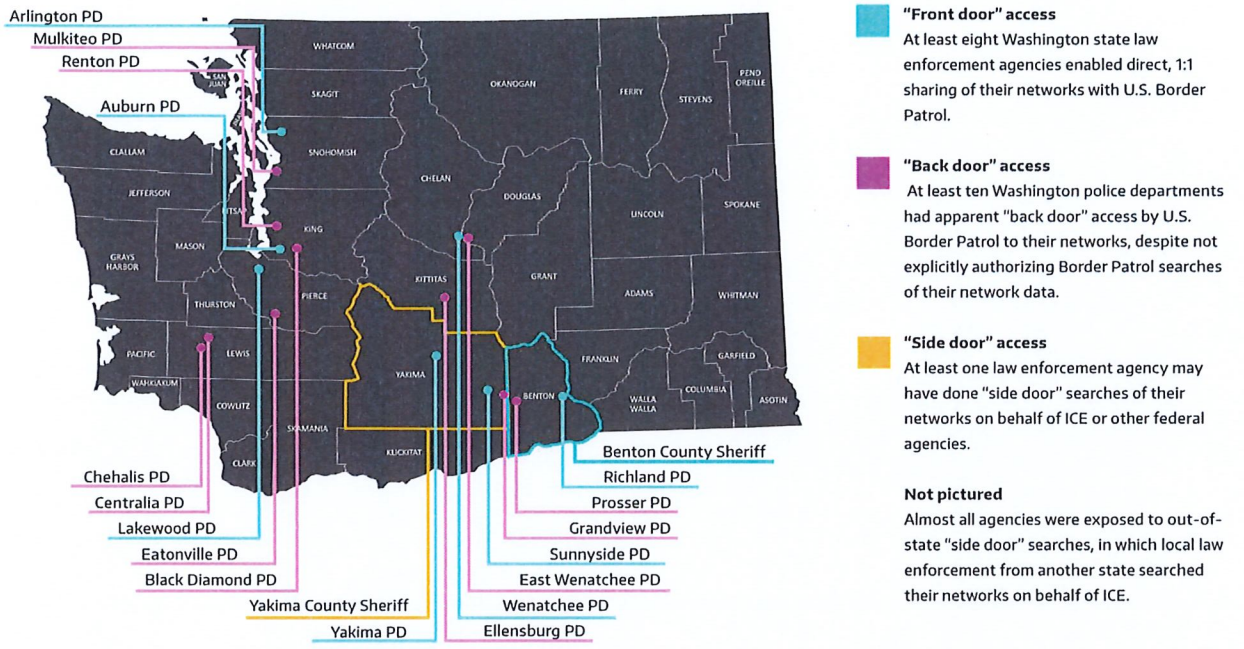
FINDINGS

Each jurisdiction that employs Flock technology creates its own "network": cameras capture images about passing cars, which Flock software then converts into data for storage, analysis and sharing. There are multiple ways for Flock organizational customers to share their data; here, we refer to them as "front door" (direct sharing of data through a 1:1 relationship with another network); "back door" (access to networks without explicit authorization by the network owner); and "side door" (searches by authorized network users on behalf of

from Kent Assistant City Attorney Logan Todd denying UW-CHR's appeal of the city's determination that Flock Network Audits do not constitute public records under Washington State's Public Records Act: see Logan Todd, email to UWCHR Research Team, August 26, 2025: https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2025/10/Flock-Report-2025-PRR-72224-Response-to-Appeal.pdf



Flock audits reveal multiple forms of access to local automated license plate reader systems by federal agencies and out of state law enforcement, including "front door" access via 1:1 sharing; "back door" access, in which records reveal searches despite direct sharing not being explicitly enabled; and "side door" access, in which local users make searches of networks to which they have access on behalf of federal immigration agencies, with keywords such as "ICE" or "immigration".



Across Washington state, a review of Flock audits by UWCHR researchers during 2025 revealed multiple forms of access to data on Washington state residents by federal immigration enforcement agencies and out-of-state law enforcement. The majority of agencies were exposed to one or more of these forms of access to their networks. The map does not depict all agencies surveyed or known to use Flock systems.

other agencies without access to the network, potentially including federal immigration enforcement agencies). For an overview of findings by agency, see the Appendix to this report.

"FRONT DOOR" ACCESS

Flock Network Sharing settings allow organizations to share access to their networks, and/or receive access to other networks on a 1:1 basis. These sharing settings are documented in Network Sharing reports; a list of "External organizations with access" may also appear on organizations' Flock Transparency Portals.

Of the agencies whose records have been reviewed to date by UWCHR, at least eight appear to have enabled 1:1 sharing with organizations identified as "U.S. Border Patrol" or "U.S. Border Patrol [Federal]" at some point during 2025. These include the Benton County Sheriff's Office and police departments in the cities of Arlington, Auburn, Lakewood, Richland, Sunnyside, Wenatchee, and Yakima.[45] All the Flock Network Audits received from these agencies show evidence of searches by U.S. Border Patrol during at least May through August 2025, as described in further detail below.

45 "U.S. Border Patrol" and "Homeland Security Investigations [Federal] [Inactive]" are listed as organizations with which Yakima PD shared Flock Network in a detailed "Network Sharing" report, which specifies that sharing with these networks began on May 19, 2025 at 6:03PM. These organizations are not listed on a less-detailed "Shared Networks" report also dated May 19, 2025; nor are they listed on an updated "Shared Networks" report dated August 30, 2025. Yakima PD Network Audits reveal searches by organizations identified as "U.S. Border Patrol" and "U.S. Border Patrol [Federal]" both before and after May 19, 2025.

1	Organization Name	Networks Shared With Me	Networks I'm Sharing
441	Peoria IL PD		Arlington WA PD,Arlington WA PD (Flex)
442	US Postal Inspection Service [Federal]		Arlington WA PD,Arlington WA PD (Flex)
443	Wyandotte MI PD		Arlington WA PD,Arlington WA PD (Flex)
444	Jackson WI PD		Arlington WA PD,Arlington WA PD (Flex)
445	TN - Lincoln County SO		Arlington WA PD,Arlington WA PD (Flex)
446	Jesup GA PD		Arlington WA PD (Flex)
447	Snohomish WA PD		Arlington WA PD,Arlington WA PD (Flex)
448	Bay St. Louis MS PD		Arlington WA PD,Arlington WA PD (Flex)
449	Lansing IL PD		Arlington WA PD,Arlington WA PD (Flex)
450	Village of Clearview WV PD		Arlington WA PD,Arlington WA PD (Flex)
451	US Border Patrol [Federal]		Arlington WA PD,Arlington WA PD (Flex)
452	Raleigh NC PD		Arlington WA PD,Arlington WA PD (Flex)
453	Chesterton IN PD		Arlington WA PD,Arlington WA PD (Flex)
454	Calhoun County SC SO		Arlington WA PD,Arlington WA PD (Flex)
455	Brevard County FL SO		Arlington WA PD,Arlington WA PD (Flex)
456	Harvey County KS SO		Arlington WA PD,Arlington WA PD (Flex)
457	Shelby County TN SO		Arlington WA PD,Arlington WA PD (Flex)
458	Iowa State University IA PD		Arlington WA PD,Arlington WA PD (Flex)
459	Ocean Springs MS PD		Arlington WA PD,Arlington WA PD (Flex)
460	Somerset County NJ Prosecutors Office		Arlington WA PD,Arlington WA PD (Flex)
461	Nebraska State Patrol		Arlington WA PD,Arlington WA PD (Flex)
462	Hope Mills NC PD		Arlington WA PD,Arlington WA PD (Flex)

Screenshot of Arlington PD Flock Network Sharing report dated July 29, 2025, detailing local networks shared with other Flock users, designated by "Organization Name". Highlighted rows show that the network had been shared with "US Border Patrol [Federal]" and "US Postal Inspection Service [Federal]", as well as hundreds of other local law enforcement organizations nationwide.

"BACK DOOR" ACCESS BY BORDER PATROL TO FLOCK NETWORKS

As noted above, in August 2025, Colorado journalists discovered that the Border Patrol had been granted access to the data generated by jurisdictions in their state who had declined to share their data with federal agencies. Flock's statements in response made it unclear whether users had opted in to sharing with the Border Patrol without realizing it, or whether the Border Patrol had been effectively granted access to the national system via a "back door."

Here in Washington, UWCHR review of Flock Network Audits uncovered similar problems. From at least May 9, 2025 through August 24, 2025, local organizations' networks were subject to thousands of searches by "US Border Patrol [Federal]". These searches were made by dozens of different users, who identified the reason for their search with terms such as "USBP", "USBP/HSI", and "immigration." While in some cases users listed search reasons that were suggestive of federal criminal investigations, such as "narcotics trafficking" or "money laundering", in others they cited exceedingly vague reasons, such as "investigation" or "targeting". According to the network audits, these searches were applied to thousands of networks and tens of thousands of devices, with searches increasing in frequency starting in May and peaking in July and August.

These searches appear in the Network Audits of at least ten Washington police departments that did not explicitly authorize Border Patrol searches of their network data: Black Diamond,

	Name	Org Name	Total Networks	Total Devices S	Time Frame	License Plate	Reason	Case #	Filters	Search Time	Search Type
183332		Washburn County WI SO	6362	84789	05/25/2025, 02:3 06/24/2025, 02:3		investigation			06/24/2025, 02:3	search
183333		Will County IL SO	6538	87660	06/22/2025, 12:5 06/23/2025, 12:5		99			06/23/2025, 12:5	lookup
183334		US Border Patrol [Federal]	6436	86171	05/24/2025, 12:5 06/23/2025, 12:5		usbp	usbp		06/23/2025, 12:5	search
183335		US Border Patrol [Federal]	6436	86171	05/24/2025, 12:5 06/23/2025, 12:5		usbp	usbp		06/23/2025, 12:5	search
183336		Hernando MS PD	6386	85287	06/16/2025, 01:0 06/23/2025, 01:0		SV			06/23/2025, 12:5	search
183337		Wilmington DE PD	5862	80625	05/25/2025, 10:2 06/24/2025, 10:2		Inv		pennsylvania	06/24/2025, 10:2	search
183338		Sarasota County FL SO	6270	82212	05/25/2025, 10:2 06/24/2025, 10:2		X31			06/24/2025, 10:2	lookup
183339		Wilmington DE PD	5862	80625	05/25/2025, 10:2 06/24/2025, 10:2		Inv		pennsylvania	06/24/2025, 10:2	search
183340		Houston TX PD	6718	86535	05/25/2025, 10:2 06/24/2025, 10:2		s			06/24/2025, 10:2	lookup
183341		Sarasota County FL SO	6270	82212	05/25/2025, 10:2 06/24/2025, 10:2		X31			06/24/2025, 10:2	lookup
183342		Auburn AL PD	6561	85817	05/24/2025, 07:1 06/23/2025, 07:1		investigative			06/23/2025, 07:1	search
183343		Williamson Co. IL SO	6529	87422	06/16/2025, 07:3 06/23/2025, 07:3		Investigative			06/23/2025, 07:1	search
183344		St. Ann MO PD	6047	81614	05/24/2025, 07:1 06/23/2025, 07:1		property damage			06/23/2025, 07:1	search

An excerpt from Renton Police Department's Flock Network Audit, obtained by UWCHR through public records requests, showing two instances of searches conducted by "US Border Patrol [Federal]" on June 23, 2025, with reason listed for search "usbp" for U.S Border Patrol. A corresponding Network Sharing report (not pictured) shows that Renton Police Department had not explicitly authorized sharing with Border Patrol.

Centralia, Chehalis, East Wenatchee, Eatonville, Ellensburg, Grandview, Mukilteo, Prosser, and Renton.

In total, Flock Network Audits show that the Border Patrol searched the ALPR data of at least 17 Washington agencies. These include sheriff's offices in Benton and Yakima counties, and police departments in the cities of Auburn, Black Diamond, Centralia, Chehalis, Eatonville, Ellensburg, Grandview, Lakewood, Mukilteo, Prosser, Renton, Richland, East Wenatchee, Wenatchee, and Yakima.

In at least six cases, including Douglas County and Kittitas County Sheriff's Offices, and the Lynnwood, Mount Vernon, and Olympia Police Departments, Flock Network Audits during 2025 do *not* contain any searches by Border Patrol, suggesting that at least some local agencies were not exposed to this "back door" access.

The details of how the Border Patrol obtained access to data generated by ALPRs in so many Washington jurisdictions remain unclear; was this the result of national "back door" access to Flock data, as 404 Media concluded, or the result of local police departments opting in to sharing with the federal agency by activating the "National Lookup" feature, as reportedly occurred in Syracuse, NY?[46] According to Flock documentation, it is activated by checking a single box in system settings, but the records released to UWCHR did not reveal whether that box had been checked by Washington jurisdictions.[47] In either case, the fact that the searches occurred raises important questions about compliance with Washington's Keep Washington Working law, which bars law enforcement agencies across the state from dedicating local resources for purposes of civil immigration enforcement.

---

46 This was cited as explanation of a similar issue in Syracuse NY: "We have communicated with Flock, and they have stated that our ALPRs were included in CBP's searches prior to June,' Coffey said. 'SPD did not enter into a data sharing arrangement with those federal agencies, but they were able to access SPD data through the National Lookup Search tool.'"

47 Gideon Epstein, "Flock Gives Law Enforcement All Over the Country Access to Your Location", ACLU of Massachusetts, October 7, 2025: https://data.aclum.org/2025/10/07/flock-gives-law-enforcement-all-over-the-country-access-to-your-location/

1	Name	Total Networks	Time Frame	License Plate	Reason	Case #	Filters	Search Time	Search Type
413	[redacted]	152	5/17/2025, 12:00:04 AM UTC 5/17/2025, 02:00:04 AM UTC	[redacted]	25C06791			5/17/2025, 01:5(	search
414	[redacted]	152	5/16/2025, 02:00:40 AM UTC 5/17/2025, 02:00:40 AM UTC	[redacted]	25C06791			5/17/2025, 01:5(	search
415	[redacted]	152	5/10/2025, 01:56:50 AM UTC 5/17/2025, 01:56:50 AM UTC	[redacted]	25C06791			5/17/2025, 01:5(	search
416	[redacted]	2	5/21/2025, 01:30:45 AM UTC 5/21/2025, 03:30:45 AM UTC	[redacted]	traffic offense	call 668		5/21/2025, 03:1(	search
417	[redacted]	133	4/21/2025, 03:13:53 AM UTC 5/21/2025, 03:13:53 AM UTC	[redacted]	traffic offense	call 668		5/21/2025, 03:1(	search
418	[redacted]	133	4/21/2025, 03:13:53 AM UTC 5/21/2025, 03:13:53 AM UTC	[redacted]	traffic offense	call 668		5/21/2025, 03:1(	search
419	[redacted]	133	4/21/2025, 03:13:00 AM UTC 5/21/2025, 03:16:00 AM UTC	[redacted]	traffic offense	call 668		5/21/2025, 03:1(	search
420	[redacted]	89	5/22/2025, 03:30:36 PM UTC 5/23/2025, 05:30:36 PM UTC	[redacted]	ICE			5/23/2025, 05:2(	search
421	[redacted]	89	5/22/2025, 03:30:52 PM UTC 5/23/2025, 05:30:52 PM UTC	[redacted]	ICE			5/23/2025, 05:2(	search
422	[redacted]	19	5/23/2025, 05:30:23 AM UTC 5/23/2025, 05:30:23 PM UTC	[redacted]	ARSON			5/23/2025, 05:2(	search
423	[redacted]	2	5/23/2025, 05:30:26 AM UTC 5/23/2025, 05:30:26 PM UTC	[redacted]	arson suspect			5/23/2025, 05:2(	search
424	[redacted]	2	5/22/2025, 05:30:47 PM UTC 5/23/2025, 05:30:47 PM UTC	[redacted]	arson suspect			5/23/2025, 05:2(	search
425	[redacted]	2	5/23/2025, 06:00:05 AM UTC 5/23/2025, 06:00:05 PM UTC	[redacted]	arson suspect			5/23/2025, 05:3(	search

A Yakima County Flock Organization Audit showing a list of network searches made by local users. Highlighted are two examples with "ICE" listed as the reason for searching the data. In each of these examples the user querying the system is an employee of Yakima Sheriff's Office. The searches were applied to 89 networks to which Yakima County Sheriff's Office had access; the identities of these networks are not specified, but corresponding searches appear in the audits of at least 10 other Washington state law enforcement agencies.

"SIDE DOOR" SEARCHES ON BEHALF OF FEDERAL IMMIGRATION ENFORCEMENT AGENCIES

UWCHR research also uncovered a third means by which local law enforcement provided ALPR data to federal immigration enforcement agencies. In other states, researchers have found that local law enforcement agencies may undertake "side door" searches on behalf of ICE or other federal agencies; this is revealed by Flock audit records listing keywords such as "ICE" or "immigration" in the system's "Reason" field.[48] In such cases, the search is conducted by the local law enforcement officer as an informal favor or act of assistance to a federal colleague. For example, in Washington, DivestSPD has reported on its blog that in June 2025, agents from Homeland Security Investigations and other agencies sent emails to law enforcement listservs asking other officers on the list to run a search on their behalf of Flock data—and that officers from multiple Western Washington jurisdictions responded by conducting the searches as requested.[49]

Public records reviewed by UWCHR researchers also uncovered one case of a "side door" search by a local law enforcement agency on behalf of ICE:[50]

- On May 23, 2025, a user with Yakima County Sheriff's Office made two searches for a timeframe of just over the preceding 24 hours with reason listed as "ICE," presumably referring to U.S. Immigration and Customs Enforcement. An Organization

48 Koebler and Cox, "ICE Taps into Nationwide AI-Enabled Camera Network, Data Shows."

49 Rose Terse, "Feds, WA police share surveillance data on an obscure SPD email list," *Divest SPD*, September 4, 2025, https://www.divestspd.com/p/feds-wa-police-share-surveillance

50 The original version of this report included mention of a January 23, 2025 search by a SeaTac police officer who listed the reason for the search as "bp"; UWCHR researchers suspected this could be a reference to Border Patrol. After the report's publication, a representative of the city of SeaTac contacted us stating that this was, in fact, a reference to the Bellevue Police, not the Border Patrol. Because Flock's safeguards against abuse rely on the assumption that law enforcement officers self-report their search reasons in good faith, UWCHR has no way to verify what "bp" referred to in this particular instance.

Audit reports that the search was applied to 89 networks. The search appears in the Network Audit records of at least 10 other local agencies including Benton County Sheriff's Office, and police departments in the cities of Auburn, Chehalis, Eatonville, Grandview, Lakewood, Mukilteo, Renton, Richland and Wenatchee.

The primary function of ICE is immigration enforcement; Washington state law restricts local and state agencies from sharing information with federal agencies for purposes of civil immigration enforcement.[51] As such, Washington law enforcement officers' active assistance of ICE in this case almost certainly constitutes a violation of Keep Washington Working.[52]

Furthermore, several other agencies made requests to other federal agencies which are not primarily involved in civil immigration enforcement, but which are currently known to be collaborating with immigration investigations and enforcement:

- Kent Police Department made searches for "HSI assist" on 1/30/25 in its own network as well as the networks of at least the Auburn, Black Diamond, Lakewood, and Renton Police Departments; and on 7/24/25 in its own network and at least the networks of the Chehalis, Centralia, Mount Vernon, and Grandview Police Departments.
- Renton Police Department made three searches in two networks on 5/13/2025 on behalf of "Special Agent Michael R. Bonner"; according to news reports[53] and court documents[54] reviewed by UWCHR, the name matches that of an HSI Special Agent.
- Richland Police made two searches for "HSI Investigation - Intel" on 4/17/2025, one targeting a single network and the other targeting 82 networks.
- Tukwila Police Department made searches for "USPIS" on 3/30/25 in its own network as well as the networks of at least the Chehalis, Mukilteo, Renton, and Auburn police departments; as well as the networks of sheriff's offices in Benton County, Yakima County, and Douglas County.
- Puyallup Police Department made searches for "USPIS" on 7/16/25 in Chehalis Police Department's Flock network and on 7/17/25 in the networks of Douglas County Sheriff's Office, Lakewood Police Department, and Renton Police Department.[55]

Homeland Security Investigations (HSI) is a DHS agency that has historically been primarily involved in investigations of crimes including terrorism, child exploitation, and drug and human trafficking, though it has also engaged in workplace raids and other acts of immigration enforcement;[56] since January 2025, however, HSI's entire investigations division—reportedly some 90% of its staff—has been diverted to assisting with deportation efforts.[57]

---

51 KWW Wash. Rev. Code § 10.93.160, https://app.leg.wa.gov/RCW/default.aspx?cite=10.93.160

52 As noted above, Flock audits do not give any indication of the results of searches, so it would be impossible to know and it is not known whether the information yielded in these searches resulted in actual immigration enforcement activities, though UWCHR has requested additional public records potentially associated with these searches.

53 Benjamin Weiser and Maria Cramer, "U.S. Says Tren de Aragua Charges Will 'Devastate' Gang's Infrastructure," New York Times, April 22, 2025, https://www.nytimes.com/2025/04/22/nyregion/federal-tren-de-aragua-charges.html

54 United States of America v. Anderson Zambrano-Pacheco, Southern District of New York, https://www.justice.gov/d9/2025-01/u.s._v._zambrano-pacheco_complaint.pdf

55 To date, Puyallup Police Department has not yet disclosed its Flock Organization Audit for July 2025, which would reflect this search in the department's own network.

56 Immigrant Legal Resource Center, National Immigrant Justice Center, and National Immigration Law Center, *Funding for ICE Homeland Security Investigations (HSI) Is Funding for Trump's Anti-Immigrant Agenda*, April 2019, https://immigrantjustice.org/sites/default/files/uploaded-files/no-content-type/2019-05/HSI-backgrounder-2019.pdf

57 Josh Meyer, "Thousands of DHS agents shift to deportation instead of drugs, weapons and human trafficking," *USA Today*, February 15, 2025, https://www.usatoday.com/story/news/politics/2025/02/14/dhs-agents-deportation-not-trafficking/78641666007/; and David J. Bier, "ICE Has Diverted Over 25,000 Officers from Their Jobs," *Cato Institute*, September 3, 2025, https://www.cato.org/blog/ice-has-diverted-over-

Name	Org Name	Total Networ	Total Device	Time Frame	License Plat	Reason	Case #	Filters	Search Time	Search Type
	Michigan State Police	6528	83741	05/19/2025, 04:3		USBP Immigrati	MIHC-2025-042	michigan	05/19/2025, 04:2	search
	Texas Department of Public S	6496	83319	03/03/2025, 12:3 05/20/2025, 11:3		ICE warrant	W646246778	Toyotatexas	05/20/2025, 11:3	search
	Michigan State Police	6528	83741	05/05/2025, 04:3 05/19/2025, 04:3		USBP Immigrati	MIHC-2025-042	michigan	05/19/2025, 04:2	search
	Michigan State Police	6528	83741	04/19/2025, 04:3 05/19/2025, 04:3		USBP Immigrati	MIHC-2025-042	michigan	05/19/2025, 04:2	search
	Lubbock County TX SO	5947	78393	04/20/2025, 08:(05/20/2025, 08:(		Immigration		texas	05/20/2025, 08:(	search
	Lubbock County TX SO	5947	78393	03/01/2025, 09:(05/20/2025, 08:(		Immigration		texas	05/20/2025, 08:(	search
	Michigan State Police	6528	83740	05/05/2025, 05:(05/19/2025, 05:(		USBP Immigrati	MIHC-2025-042	michigan	05/19/2025, 04:4	search
	Michigan State Police	6528	83742	05/05/2025, 05:(05/19/2025, 05:(		USBP Immigrati	MIHC-2025-042	michigan	05/19/2025, 04:4	search
	Michigan State Police	6528	83742	05/05/2025, 05:(05/19/2025, 05:(		USBP Immigrati	MIHC-2025-042	michigan	05/19/2025, 04:5	search
	Michigan State Police	6528	83742	05/05/2025, 05:(05/19/2025, 05:(		USBP Immigrati	MIHC-2025-042	michigan	05/19/2025, 04:5	search
	Florida Highway Patrol	6540	83451	04/19/2025, 05:1 05/19/2025, 05:1		ice		florida	05/19/2025, 05:1	lookup
	Florida Highway Patrol	6540	83454	04/19/2025, 05:2 05/19/2025, 05:2		ice		florida	05/19/2025, 05:2	lookup
	Florida Highway Patrol	6540	83440	04/19/2025, 01:5 05/19/2025, 01:5		ice		florida	05/19/2025, 01:5	lookup
	Yakima County WA SO	89	1124	05/22/2025, 03:3 05/23/2025, 05:3		ICE			05/23/2025, 05:2	search
	Yakima County WA SO	89	1124	05/22/2025, 03:3 05/23/2025, 05:3		ICE			05/23/2025, 05:2	search
	Lafayette Parish LA SO	5880	78509	04/28/2025, 04:1 05/28/2025, 04:1		ice investigation			05/28/2025, 06:1	search
	Lafayette Parish LA SO	5880	78509	05/21/2025, 06:3 05/28/2025, 06:3		ice investigation			05/28/2025, 06:1	search
	Lafayette Parish LA SO	5880	78509	05/21/2025, 06:3 05/28/2025, 06:3		ice investigation			05/28/2025, 06:1	search
	Florida Highway Patrol	6509	83800	04/29/2025, 09:5 05/29/2025, 09:5		ice		florida	05/29/2025, 09:5	lookup

Screenshot of a May, 2025 Network Audit for Renton Police Department's Flock system, depicting dozens of searches of the local network for reasons including "ICE" and "immigration" by Yakima County Sheriff's Office and law enforcement agencies from around the country.

Similarly, the U.S. Inspection Service (USPIS), the law enforcement branch of the U.S. Postal Service, is not primarily responsible for immigration enforcement, but has reportedly been enlisted as a source of targeting for immigration enforcement in recent months.[58,59] In addition, because of data-sharing across networks, Washington drivers' data has been exposed to numerous "side door" searches by law enforcement agencies across the country, including thousands of searches with "Reason" listed as "immigration", "ICE", "ERO", "criminal alien", and other similar terms. Such searches appear in the Network Audits of the sheriff's offices in Benton, Douglas, and Yakima Counties; and of police departments in the cities of Auburn, Black Diamond, Centralia, Chehalis, East Wenatchee, Eatonville, Ellensburg, Grandview, Lakewood, Lynnwood, Mukilteo, Prosser, Renton, Richland, Wenatchee, and Yakima from January through August, 2025.

Only three jurisdictions appear to have maintained Flock networks without any documented exposure to either "back door" searches by U.S. Border Patrol or "side door" searches by other local law enforcement agencies: Kittitas County Sheriff's Office,[60] Mount Vernon Police Department, and Olympia Police Department. These jurisdictions appear to share the common characteristic of restricting network access to law enforcement agencies in Washington state only.

25000-officers-their-jobs

58 Jacob Bogage and Hannah Natanson, "USPS law enforcement assists Trump 'mass deportation' effort, sources and records show," *Washington Post*, April 29, 2025, https://www.washingtonpost.com/business/2025/04/29/usps-immigration-trump-deportations/; and Elizabeth Crisp, "Postal Service joins Trump administration immigration enforcement effort," *The Hill*, April 30, 2025, https://thehill.com/homenews/5275616-usps-joins-efforts-illegal-immigration/

59 USPIS is one of a limited number of federal agencies with which several Washington Flock customers share data on a 1:1 basis according to Network Sharing reports and Transparency Portals; see the Appendix to this report.

60 Kittitas County Sheriff's Office only disclosed one month of Flock Network Audit data for June 29 through July 30, 2025.

DISCREPANCY BETWEEN FLOCK AUDITS AND ACCESS SETTINGS

In addition to the specific concerns noted above, UWCHR researchers have noted broad discrepancies between the contents of Flock audits and documentation of organizations' network access settings.

In many cases, Flock Network Audits revealed thousands of searches of local organizations' networks by other organizations which do not appear in either their Network Sharing report lists of "Networks I'm Sharing With" or Transparency Portal lists of "External organizations with access". As noted above, this may be explained if local organizations have opted in to Flock's "National lookup" capability, but if so, this is not clearly delineated by the contents of the Network Audits themselves.

In addition, Flock users appear to have the ability to search more networks than those identified as having been directly shared with their organizations. In all but two cases among those reviewed by UWCHR, Flock Organization Audit reports record agencies making searches across a greater number of networks than those listed in their respective Network Sharing reports. For example, Renton Police Department's Network Sharing report lists 91 other organizations in its "Networks shared with me" column, while the department's Flock Organization Audit reports searches across up to 6511 networks and tens of thousands of devices. Flock's Organization Audit reports do not offer any information about the identity of the networks searched by a given organization, only the number of networks and devices searched. For example, it is impossible to determine whether these include public or private networks.

In just one case, Yakima Police Department, the agency's Flock Network Sharing report included additional columns not present in records disclosed by other agencies, including "Organization Owner Type" and the dates that networks were first shared. This is also the only Network Sharing report reviewed by UWCHR which includes private and business networks among those shared with a local law enforcement agency, including several operated by a local property management company, and 92 Lowe's hardware stores, including out of state locations.[61] It is not clear whether Yakima Police Department's access to these private networks is an outlier, or whether such access is more common but other jurisdictions have failed to disclose these categories in their Flock Sharing reports.

For these reasons, it is currently impossible for independent researchers to definitively determine the scope of local Flock network users' access to, or exposure to, other organizations with Flock network access, and it may be challenging for system administrators themselves to understand the implications of the settings they have activated on their network. This is particularly worrisome given the shifting and sometimes inaccurate statements made by Flock about its product's sharing features.

---

61 Koebler, "Home Depot and Lowe's Share Data From Hundreds of AI Cameras With Cops."

1	Organization Owner	Organization Owner Type	Network Name	Network CSM	Organization Shared With	Organization Shared With Type	First Shared With Organization
78	Lowe's Corporation	business	Lowe's #0018	[redacted]	Yakima WA PD	lawEnforcement	8/16/2024 16:49:44
79	Lowe's Corporation	business	Lowe's - #0152	[redacted]	Yakima WA PD	lawEnforcement	8/16/2024 16:49:44
80	Lowe's Corporation	business	Lowe's - #0172	[redacted]	Yakima WA PD	lawEnforcement	8/16/2024 16:49:44
81	Lowe's Corporation	business	Lowe's - #0249	[redacted]	Yakima WA PD	lawEnforcement	8/16/2024 16:49:45
82	Lowe's Corporation	business	Lowe's - #0319	[redacted]	Yakima WA PD	lawEnforcement	8/16/2024 16:49:44
83	Lowe's Corporation	business	Lowe's - #1904	[redacted]	Yakima WA PD	lawEnforcement	8/16/2024 16:49:45
84	Lowe's Corporation	business	Lowe's - #1905	[redacted]	Yakima WA PD	lawEnforcement	8/16/2024 16:49:44
85	Lowe's Corporation	business	Lowe's - #1906	[redacted]	Yakima WA PD	lawEnforcement	8/16/2024 16:49:45
86	Lowe's Corporation	business	Lowe's - #2344	[redacted]	Yakima WA PD	lawEnforcement	8/16/2024 16:49:44
87	Lowe's Corporation	business	Lowe's - #2573	[redacted]	Yakima WA PD	lawEnforcement	8/16/2024 16:49:45
88	Lowe's Corporation	business	Lowe's - #2587	[redacted]	Yakima WA PD	lawEnforcement	8/16/2024 16:49:44
89	Lowe's Corporation	business	Lowe's - #2597	[redacted]	Yakima WA PD	lawEnforcement	8/16/2024 16:49:46
90	Lowe's Corporation	business	Lowe's - #2608	[redacted]	Yakima WA PD	lawEnforcement	8/16/2024 16:49:44
91	Lowe's Corporation	business	Lowe's - #2956	[redacted]	Yakima WA PD	lawEnforcement	8/16/2024 16:49:44
92	Lowe's Corporation	business	Lowe's - #3045	[redacted]	Yakima WA PD	lawEnforcement	8/16/2024 16:49:44
93	Lowe's Corporation	business	Lowe's - #3206	[redacted]	Yakima WA PD	lawEnforcement	8/16/2024 16:49:44
94	Lowe's Corporation	business	Lowe's - #3240	[redacted]	Yakima WA PD	lawEnforcement	8/16/2024 16:49:45
95	Lowe's Corporation	business	Lowes - #0004	[redacted]	Yakima WA PD	lawEnforcement	8/16/2024 16:49:44
96	Lowe's Corporation	business	Lowes - #0010	[redacted]	Yakima WA PD	lawEnforcement	8/16/2024 16:49:44
97	Lowe's Corporation	business	Lowes - #0026	[redacted]	Yakima WA PD	lawEnforcement	8/16/2024 16:49:44
98	Lowe's Corporation	business	Lowes - #0035	[redacted]	Yakima WA PD	lawEnforcement	8/16/2024 16:49:44
99	Lowe's Corporation	business	Lowes - #0061	[redacted]	Yakima WA PD	lawEnforcement	8/16/2024 16:49:44

An excerpt from Yakima Police Department's Flock network sharing settings, dated May 19, 2025, listing the hardware store Lowe's as a business organization that shares Flock network data for locations nationwide with Yakima Police Department.

CONCLUSIONS

Washington currently has no law regulating the appropriate use of ALPR technology, though some other states have passed related laws. California, for example, bars ALPR data sharing across state lines;[62] Virginia restricts ALPR use to investigations in a limited set of criminal matters;[63] and Illinois requires that out-of-state law enforcement agencies seeking to access data collected in Illinois first attest in writing that the data would not be used to enforce other states' laws on abortion or immigration.[64] However, research suggests all three of these laws are regularly violated.[65]

Privacy advocates warn that the proliferation of ALPR technology threatens the rights protected by the Fourth Amendment to the U.S. Constitution, which bars unreasonable searches and seizures.[66] While promoters of ALPRs, on the other hand, suggest there is no reasonable expectation of privacy for activities, like driving, which are conducted in public space, and therefore that searching data generated by such movements is not an undue infringement on anyone's rights, the reach of new technology allows law enforcement to amass an astounding degree of information about individuals' lives.

The Electronic Frontier Foundation warns, "By matching your car to a particular time, date, and location, and then building a database of that information over time, law enforcement can learn where you work and live, what doctor you go to, which religious services you attend, and who your friends are." And by applying algorithms to this data, "systems can reveal regular travel patterns and predict where a driver may be in the future."[67]

62 Flock Safety, "Setting the Record Straight: Statement on Flock Network Sharing, Use Cases, and Federal Cooperation."

63 Alex Littlehales and Kyle Johnson, "Youngkin signs bill placing regulations on license plate readers and law enforcement," *13News Now*, May 5, 2025, https://www.13newsnow.com/article/news/local/virginia/youngkin-virginia-bill-license-plate-reader-law-enforcement-regulations/291-5368d054-23cf-417f-a000-58c3b22786b8

64 Andrew Adams, "Illinois license plate cameras used illegally by out-of-state police, Giannoulias says," *Capitol News Illinois*, June 12, 2025, https://capitolnewsillinois.com/news/illinois-license-plate-cameras-used-illegally-by-out-of-state-police-giannoulias-says/

65 In California, see Khari Johnson and Mohamed Al Elew, "California police are illegally sharing license plate data with ICE and Border Patrol," *Cal Matters*, June 13, 2025, https://calmatters.org/economy/technology/2025/06/california-police-sharing-license-plate-reader-data/; in Illinois, see Adams, "Illinois license plate cameras used illegally by out-of-state police, Giannoulias says."; in Virginia, see Falayi, "The feds' hidden immigration weapon: Virginia's surveillance network."

66 Jennifer Lynch, "EFF Urges Virginia Court of Appeals to Require Search Warrants to Access ALPR Databases," *Electronic Frontier Foundation*, September 29, 2025, https://www.eff.org/deeplinks/2025/09/eff-urges-virgina-court-appeals-require-search-warrants-access-alpr-databases

67 "Street-Level Surveillance: Automated License Plate

The proliferation of these technologies impacts the rights of all Washingtonians. And at a time when many of our neighbors are being subjected to raids by federal immigration authorities, which may result in fates as dire as their being forcibly disappeared,[68] Washingtonians expect that our government exercise particular caution in sharing data with the federal agencies involved in such abuses. On September 29, Governor Ferguson issued an Executive Order affirming the importance of handling immigrant Washingtonians' private data with care.[69] The order is primarily directed at state-level agencies, whereas the ALPRs discussed here are owned by local governments, but the order reaffirms the importance of responsible management of data and establishes an Immigration Sub-Cabinet "tasked with coordinating on immigration and related issues such as data privacy, health care, the bipartisan Keep Washington Working Act, and other programs or services concerning immigrant rights and interests."[70]

In this context, the findings shared here are important to take seriously. At minimum, Washingtonians deserve to know whether law enforcement agencies using Flock ALPRs—as well as surveillance technology offered by other companies—are complying with state law, including Keep Washington Working. We deserve full information about whether the businesses we patronize and the governments we elect are selling data about us to private companies, or sharing it with federal agencies and out-of-state law enforcement who may use it to target us or our neighbors. And on the basis of that information, Washingtonians deserve a robust public discussion about the degree to which we authorize the use of these technologies in our communities.

Readers (ALPRs)," *Electronic Frontier Foundation*, August 28, 2017, https://www.eff.org/pages/automated-license-plate-readers-alpr.

68 University of Washington Center for Human Rights, *Gross Human Rights Violations in Washington State: Enforced Disappearance and Refoulement*, August 21, 2025, https://jsis.washington.edu/humanrights/2025/08/21/gross-human-rights-violations-in-washington-state-enforced-disappearance-and-refoulement/

69 Executive Order 25-09, "Reaffirming Washington's Commitment to Protecting the Rights and Interests of Immigrant Communities," State of Washington Office of Governor Bob Ferguson, September 25, 2025, https://governor.wa.gov/sites/default/files/exe_order/25-09%20-%20Protecting%20Immigrant%20Communities%20%28tmp%29.pdf

70 Office of Bob Ferguson, "Governor Ferguson signs Executive Order reaffirming Washington's commitment to protecting immigrant rights," September 29, 2025, https://governor.wa.gov/news/2025/governor-ferguson-signs-executive-order-reaffirming-washingtons-commitment-protecting-immigrant

APPENDIX

TABLE: FLOCK AUDIT FINDINGS

Agency	Non-WA organizations in Shared Networks report?	Federal orgs. in Shared Networks report?	Network Audit months	USBP searches in Network Audits?	Other immigration-related searches in Network Audits?
Benton County Sheriff's Office	Yes	USBP, USPIS	Jan. - July 2025	Yes	Yes
Douglas County SO	Yes	None	March - July 2025	No	Yes
Kittitas County SO	Yes	USPIS	July 2025	No	No
Auburn Police Department	Yes	USBP, USPIS	Jan. - July 2025	Yes	Yes
Black Diamond PD	Yes	USPIS	Jan. - August 2025	Yes	Yes
Centralia PD	Yes	None	Jan. - August 2025	Yes	Yes
Chehalis PD	Yes	None	Jan. - August 2025	Yes	Yes
East Wenatchee PD	Yes	USPIS	July - August 2025	Yes	Yes
Eatonville PD	Yes	None	Dec. 2024 - July 2025	Yes	Yes
Ellensburg PD	Yes	USPIS	Jan. - July 2025	Yes	Yes
Grandview PD	Yes	USPIS	Jan. - July 2025	Yes	Yes
Lakewood PD	Yes	USPIS, USBP	Jan. - July 2025	Yes	Yes
Lynnwood PD	No	None	July - mid-August 2025	No	Yes
Mount Vernon PD	No	None	Jan. - July 2025	No	No
Mukilteo PD	Yes	None	Jan. - July 2025	Yes	Yes
Olympia PD	No	None	Jan. - July 2025	No	No
Prosser PD	No	None	Dec. 2024 - May 2025	Yes	Yes
Renton PD	No	None	Jan. - August 2025	Yes	Yes

Richland PD	Yes	USBP, USPIS	Jan. - July 2025	Yes	Yes
Wenatchee PD	Yes	USBP	Jan. - August 2025	Yes	Yes
Yakima PD*	Yes - Including private networks	USBP, USPIS, HSI	Dec. 2024 - May 2025	Yes	Yes
* "U.S. Border Patrol" and "Homeland Security Investigations [Federal] [Inactive]" are listed as organizations with which Yakima PD shared Flock Network in a detailed "Network Sharing" report, which specifies that sharing with these networks began on May 19, 2025 at 6:03PM. These organizations are not listed on a less-detailed "Shared Networks" report also dated May 19, 2025; nor are they listed on an updated "Shared Networks" report dated August 30, 2025.					
Agencies for which UWCHR lacks complete data					
Kitsap County SO	No	None	*No local Flock hardware*		
Yakima County SO	*Shared Networks report disclosure pending*		Jan. - July 2025	Yes	Yes
Arlington PD	Yes	USPIS, USBP	*Network Audits denied*		
Everett PD	Yes	None	*Network Audits denied*		
Kent PD	Yes *(per Transparency Portal; Shared Networks not disclosed)*	USPIS, USMS *(Per Transparency Portal)*	*Network Audits denied*		
Medina PD	Yes	None	*Network Audits denied*		
Monroe PD	No	None	*No local Flock hardware*		
Sedro-Wooley PD	Yes	USPIS	*Network Audits pending*		
Sunnyside PD	Yes	USBP, USPIS	*Network Audits not disclosed*		
Tukwila PD	Yes	None	*Network Audits denied*		
UWCHR requests for public records are pending from the following agencies: Napavine PD, Puyallup PD, Snohomish County Sheriff's Office, Spokane County Sheriff's Office, Spokane PD, Airway Heights PD, and King County Sheriff's Office (King County Sheriff's Office itself does not have a Flock contract, but is responsible for public disclosure for the police departments of Covington, Newcastle, and SeaTac, which do employ Flock systems). UWCHR researchers also consulted and are grateful for the following public records requests filed by Rose Terse and made public via Muckrock: Prosser PD, Medina PD, Tukwila PD, Yakima PD (published on May 14, 2025); and Ellensburg PD, Centralia PD (published on May 22, 2025).					



Leaving the Door Wide Open:
Flock Surveillance Systems Expose Washington Data to Immigration Enforcement

Center for Human Rights
The Henry M. Jackson School of International Studies
University of Washington
Box 353650, Seattle, WA 98195-3650
Phone: (206) 685-3435 | Email: uwchr@uw.edu
www.jsis.washington.edu/humanrights

Shared DATA File

Organization Name	Networks Shared With Me	Networks I'm Sharing
Monroe County MI SO	Monroe County MI SO	Pentwater MI PD
Sylvania OH PD	Sylvania OH PD	
Romulus MI PD	Romulus MI PD (LPR)	Pentwater MI PD
Zeeland MI PD	Zeeland MI PD	Pentwater MI PD
Reedsburg WI PD	Reedsburg WI PD	
Mattoon IL PD	Mattoon IL PD	
Richland County WI SO	Richland County WI SO	
Middlebury IN PD	Middlebury IN PD	
[Federal] Indiana Dunes National Par	Indiana Dunes National Park IN PD	
Florissant MO PD	Florissant MO PD	
Wyoming MI PD	Wyoming MI PD	Pentwater MI PD
Southfield MI PD	Southfield MI PD	Pentwater MI PD
Springdale OH PD	Springdale OH PD	
Birmingham MI PD	Birmingham MI PD	
Melvindale MI PD	Melvindale MI PD Condors	Pentwater MI PD
Belpre OH PD	Belpre OH PD	
Westland MI PD	Westland MI PD	Pentwater MI PD
Armada MI PD	Armada MI PD	
Garden City MI PD	Garden City MI PD	Pentwater MI PD
Clinton Township MI PD	Clinton Township MI PD	Pentwater MI PD
Kent County MI SO	Kent County MI SO	Pentwater MI PD
Monroe County WI SO	Monroe County WI SO	
Flint MI PD	Flint MI PD	Pentwater MI PD
Oceana County MI SO	Oceana County MI SO	Pentwater MI PD
Monroe MI PD	Monroe MI PD,Monroe MI PD Condors	Pentwater MI PD
Wauwatosa WI PD	Wauwatosa WI PD	
Villa Park IL PD	Villa Park IL PD (flex),Villa Park IL PD	
Waterford Township MI PD	Waterford Township MI PD	Pentwater MI PD
Winnebago County WI SO	Winnebago County WI SO	
Jackson MI PD	Jackson MI PD	Pentwater MI PD
Muskegon Heights MI PD	Muskegon Heights MI PD Condors,Muskegon Heights M	Pentwater MI PD

Tinley Park IL PD	Tinley Park IL PD,Tinley Park IL PD Flex	
Muskegon Township MI PD (Muskegor	Muskegon Township MI PD (Muskegon County)	Pentwater MI PD
Griffith IN PD	Griffith IN PD	
St. Joseph Department of Public Safet	Saint Joseph MI DPS	
Macomb County MI SO	Macomb County MI SO,Macomb County MI SO (Flex)	Pentwater MI PD
MI - Village of Middleville	Village of Middleville PD MI	Pentwater MI PD
Redford Twp MI PD	Redford Twp MI PD	
Novi MI PD	Novi MI PD	Pentwater MI PD
Fruitport Township MI PD	Fruitport Township MI PD (LPR)	Pentwater MI PD
IN - Angola PD	Angola PD IN	
Hancock County IN SO	Hancock County IN SO	
Schuyler Co. IL SO	Schuyler Co. IL SP	
Calhoun County MI SO	Calhoun County MI SO (FLEX),Calhoun County MI SO	Pentwater MI PD
Waukesha County WI SO	Waukesha County WI SO	
New Haven IN PD	New Haven PD IN	
White Lake Twp MI PD	White Lake Twp MI PD	Pentwater MI PD
Clio MI PD	Clio MI PD	Pentwater MI PD
Clawson MI PD	Clawson MI PD	Pentwater MI PD
Farmington Hills MI PD	Farmington Hills MI PD	Pentwater MI PD
Grand Traverse County MI SO	Peninsula Twp,Grand Traverse Co SO - FLEX,East Bay T	Pentwater MI PD
Eastpointe MI PD	Eastpointe MI PD	Pentwater MI PD
Northville Twp MI PD	Northville Twp MI PD	Pentwater MI PD
Crawfordsville IN PD	Crawfordsville IN PD	
Ottawa County MI SO	Ottawa County MI SO	Pentwater MI PD
Highland IN PD	Highland IN PD	
Rochester MI PD	Rochester MI PD (FLEX)	
Sawyer County WI SO	Sawyer County WI SO	
Taylor MI PD	Taylor MI PD (CONDOR),Taylor MI PD	Pentwater MI PD
St. Clair County MI SO	St. Clair County MI SO	Pentwater MI PD
Crown Point IN PD	Crown Point IN PD	
Elkhart PD IN	Elkhart IN PD	
West Bend WI PD	West Bend WI PD	
Lincoln Park MI PD	Lincoln Park MI PD	Pentwater MI PD

Van Buren MI PD	Van Buren Township MI PD	Pentwater MI PD
Jackson County MI SO	Jackson County MI SO	Pentwater MI PD
Trenton PD MI	Trenton MI PD	Pentwater MI PD
Hobart IN PD	Hobart IN PD	
Mauston WI PD	Mauston WI PD	
Grandville PD MI	Grandville MI PD	
Porter County IN SO	Porter County IN SO	
Fairfax OH PD	Fairfax OH PD,Fairfax OH PD (Live View)	
Springport Twp MI PD	Springport Twp MI PD	Pentwater MI PD
Eaton Rapids MI PD	Eaton Rapids MI PD	
Utica MI PD	Utica MI PD	Pentwater MI PD
Watertown WI PD	Watertown WI PD	
Nottawaseppi Huron Band of the Pota	Nottawaseppi Huron Band of the Potawatomi Tribal Police MI	
Berrien County MI SO	Berrien County MI SO	Pentwater MI PD
Brookfield WI PD	Brookfield WI PD	
RIG WI DTF	RIG WI DTF	
St. Clair MI PD	St. Clair MI PD	Pentwater MI PD
Portage WI PD	Portage WI PD	
Warren MI PD	Warren MI PD	Pentwater MI PD
Bloomfield Twp MI PD	Bloomfield Twp MI PD	Pentwater MI PD
Charlotte MI PD	Charlotte MI PD	Pentwater MI PD
Shelby Township MI PD	Shelby Township MI PD	Pentwater MI PD
Kalamazoo Township MI PD	Kalamazoo Township MI PD	
Auburn Hills MI PD	Auburn Hills MI PD	Pentwater MI PD
Chesterfield Twp MI PD	Chesterfield MI PD	Pentwater MI PD
Flat Rock MI PD	Flat Rock MI PD	
Cass County MI SO	Cass County MI SO	Pentwater MI PD
Roseville MI PD	Roseville MI PD	Pentwater MI PD
Gun Lake Tribal PD MI	Gun Lake Tribal PD MI	Pentwater MI PD
Marysville MI PD	Marysville MI PD	Pentwater MI PD
Sumpter Twp MI PD	Sumpter Twp MI PD	Pentwater MI PD
Milford MI PD	Milford MI PD	Pentwater MI PD
Ironwood PSD MI	Ironwood PSD MI	

Fraser MI DPS	Fraser MI DPS	Pentwater MI PD
Racine WI PD	Racine WI PD	
Elm Grove WI PD	Elm Grove WI PD	
Bridgeport Township MI PD	Bridgeport Twp PD MI	Pentwater MI PD
Antrim County SO MI	Antrim County MI SO	Pentwater MI PD
Brown Deer WI PD	Brown Deer WI PD	
Richland Village MI PD	Richland Village MI PD	Pentwater MI PD
Wolverine Lake MI PD	Wolverine Lake MI PD	Pentwater MI PD
Metro Police Authority of Genesee Co	Metro Police Authority of Genesee County	Pentwater MI PD
Holland MI PD	Holland MI PD	Pentwater MI PD
New Chicago IN PD	New Chicago IN PD	
Muskegon County MI SO	Muskegon County MI SO	Pentwater MI PD
Lathrup Village MI PD	Lathrup Village MI PD	Pentwater MI PD
Muskegon MI PD	Muskegon MI PD	Pentwater MI PD
Lapeer City MI PD		Pentwater MI PD
Michigan Department of Corrections (MDOC)		Pentwater MI PD
Saint Clair Shores MI PD		Pentwater MI PD
Oak Park MI Dept of Public Safety		Pentwater MI PD
Dickinson County MI SO		Pentwater MI PD
Livonia MI PD		Pentwater MI PD
Inkster MI PD		Pentwater MI PD
Beverly Hills MI PD		Pentwater MI PD
Schoolcraft College MI PD		Pentwater MI PD
Woodhaven MI PD		Pentwater MI PD
Metamora Township MI PD		Pentwater MI PD
Port Huron MI PD		Pentwater MI PD
Western Michigan University MI PD		Pentwater MI PD
Lansing MI PD		Pentwater MI PD
Menominee County SO MI		Pentwater MI PD
South Lyon MI PD		Pentwater MI PD
Saginaw Valley State University MI PD		Pentwater MI PD
Michigan Department of Natural Resources		Pentwater MI PD
East Lansing MI PD		Pentwater MI PD