Dear City Councilmembers,

Happy holidays and happy new year. My name is Fletcher Crone, a former longtime resident of Whitewater. I am writing to you with concern about the recent proliferation of Flock Safety surveillance cameras within Whitewater. I grew up in Whitewater, my parents, brother, and grandparents all live in Whitewater, and I am highly concerned about the impact that Flock cameras might have on the local community and my family.

Before I get into the reasons behind those concerns, I would like to say that I do very much understand the excitement surrounding their implementation. If the City of Whitewater was pitched that Flock cameras solved 10% of nationwide crime, and resulted in an up to 70% reduction in crime in certain communities, it's obvious to see why Flock Safety seemed like a silver bullet solution. However, according to reporting from Forbes and 404 Media, their claims of widespread crime reduction are downright false and misleading. Forbes showed that crime has actually increased in the community where Flock claimed a 70% decrease. To date, there have been no conclusive and comprehensive studies which show that Flock's cameras decrease crime.

Beyond the company's false claims, I have two main concerns regarding use of their cameras which I feel are strong enough to warrant their removal.

First, I'd like to address their main advertised purpose; catching criminals. Many people have posed the question: "If you aren't committing any crimes, what do you have to worry about?" It turns out, there is a lot to worry about. According to data from the Northern California Regional Intelligence Center, Flock Cameras have been wrong 1 in 10 times. There have been numerous cases across the country in which families and individuals have been held at gunpoint or handcuffed because License Plate Reader cameras simply misidentify the plate or individual associated with it (1)(2)(3). A $1.9 million dollar lawsuit was recently settled in Colorado for a family with small children who were held at gunpoint because a camera misidentified their license plate. With a 10% failure rate, it seems that it is only a matter of time before Flock Cameras lead to the wrongful detention of an innocent family in Whitewater.

We can also ask the question, what if you are a "criminal"? There have been countless examples of Flock Cameras being used by ICE, CBP, and DHS agents to target, arrest, and deport undocumented immigrants. As we all know, Whitewater is a city filled with immigrants, many of whom are in the country illegally. While none of those agencies have direct access to the network of Flock cameras, the company itself has acknowledged that CBP has accessed 82,000 Flock cameras through data-sharing agreements with local police departments. This means that nearly every Flock camera in the nation is accessible to CBP. Have Whitewater's 13 cameras been used against our immigrant community? Do we even have a way of knowing if or when they are used by CBP?

Along with these data-sharing agreements, it has been shown that local departments have been conducting searches of the Flock database on behalf of ICE. Just a few hours south of

Whitewater, Danville, Illinois cameras were searched by police departments from all across the U.S. with search reasons including “immigration,” “ICE,” and “ICE+ERO,” meaning ICE Enforcement and Removal Operations. In a similar vein, an analysis of Flock queries done by the Wisconsin Examiner found that the top two reasons listed for searches of their system were “investigation” and “inv,” accounting for 30,000 searches. This further shows a lack of transparency around the use of Flock’s database which could be exploited by departments conducting searches on behalf of ICE.

Aside from immigration, Flock cameras have been used to track people for getting abortions that are illegal in their home state. Documents obtained by the Electronic Frontier Foundation show that Flock cameras from across the country were accessed under the reason “had an abortion, search for female” as part of an investigation into a “death investigation.” I do assume that Whitewater intends to use their network of Flock cameras to help solve trafficking crimes and property crimes, but with these examples, it isn’t clear if the city can prevent other agencies and departments from using their cameras for purposes that don’t align with our laws and morals.

Another reason that I strongly oppose the use of these cameras is the myriad security vulnerabilities that Flock has been exposed as having, some of which are hilariously glaring. Again reported on by 404 Media, one such vulnerability included the exposure of at least 60 cameras’ live feeds and administrator control panels (including the ability to download 30 days of camera footage and change camera settings) to the open internet without any sort of security. These control panels were publicly available, and spanned cameras from coast to coast. Technology researcher Benn Jordan unearthed feeds which included farmers markets and even children’s playgrounds. Jordan even demonstrated how footage security vulnerabilities like these could be abused with commercially available investigation technologies to identify the people in the video feeds.

These public feeds are just the tip of the iceberg. Further research from Jordan and cybersecurity researcher John Gaines revealed nearly 50 security issues related to Flock Safety cameras and their databases. To list just a handful of these issues, we can get a picture of a wholly vulnerable, dangerously exposed public surveillance system. Firstly, there is the documented sale of law enforcement Flock Safety accounts, allowing bad actors to purchase access to the entire network of Flock cameras and their databases.

Another vulnerability involved the ability to obtain direct access to the devices through a series of button presses on the Flock Falcon camera, which causes the device to put out a wifi signal which can be connected to, and through which one can access the files and programs on the camera. All of this can be done within mere seconds. In a video detailing this, and other vulnerabilities, Benn Jordan explains how access to a Flock camera and its files could theoretically be used to replace or modify footage or images taken by the camera, calling into question the legitimacy of their use in court. In that same video, Jordan points out that access to the Flock system doesn’t even require law enforcement to use Two-Factor Authentication. This glaring vulnerability has led U.S. Senator Ron Wyden to request an FTC investigation into the *company on the grounds of national security. I highly recommend watching Jordan's video to get a clear demonstration and explanation of the many basic security vulnerabilities that are present in Flock Safety's ecosystem.*

It is my hope that the City of Whitewater and the Whitewater Police Department take the time to reconsider the adoption and expansion of Flock technology. In our current political climate, it seems to me irresponsible to proliferate a technology of mass surveillance which has so many times been used to target immigrants, with and without the approval of local law enforcement. It further seems irresponsible to continue to use Flock's products when they have been routinely exposed for more-than-horrible security practices. I welcome further discussion on the topic as you consider what I have presented.

Best,
Fletcher Crone

fletchercrone@gmail.com

—---

We understand communities may have concerns about public safety technology and take them seriously. Oftentimes, we find these concerns are rooted in misinformation and lack of understanding of the Flock system. Flock Safety prides itself on being a company that was built with privacy in mind and one that supports transparency and ethical use. We appreciate the opportunity to provide an overview of the Flock LPR system and factual information.

LPR Overview

Flock's License Plate Recognition (LPR) technology captures point-in-time images of license plates and vehicle details—such as make, type, and color—on public roadways from fixed locations. They do not follow a vehicle from origin to destination, cover only a small fraction of a city's roads, and provide samples, not a seamless diary of one's movements. The system gathers objective evidence related to vehicles, not individuals, and helps law enforcement identify and locate vehicles connected to criminal investigations.

When a captured plate matches a known hot list (e.g., stolen vehicles, AMBER Alerts), Flock's system can automatically alert law enforcement in real time. This allows agencies to respond quickly and effectively.

Flock's LPR is designed with public accountability and privacy in mind:

- Not facial recognition technology
- Not tied to names, dates of birth, Social Security numbers, or addresses
- Not used for monitoring speed or issuing traffic citations
- Complies with all applicable state laws and data regulations

Data is automatically deleted after thirty (30) days by default, unless a longer retention is required by the customer. This technology provides law enforcement with reliable, time-sensitive evidence to support crime prevention and investigation—while prioritizing transparency and privacy protection.

Impact

At Flock Safety, we measure our success by the real-world outcomes our law enforcement partners achieve in solving crimes and keeping their communities safe. We work to track outcomes our customers report in real criminal investigations and the recovery of missing persons.

Flock's LPR technology has been endorsed by the National Center for Missing and Exploited Children (NCMEC) as a highly effective tool helping recover missing persons. LPRs have been used by law enforcement to safely recover well over 1,000 missing persons, with more than 100 confirmed cases of safely recovered missing children. You can find attached a letter from NCMEC highlighting why LPRs are important tools for law enforcement in quickly and effectively responding to AMBER Alerts.

The following are just a few examples of how agencies locally and nationwide have used Flock to enhance public safety in their communities:

- An MIT professor was killed — and the suspect was found using Flock's technology.
- Flock cameras used to find missing Clyde man with dementia
- Fairfax Real Time Crime Center locates missing couple with dementia in North Carolina
- Police Use Tech To Find Missing Elderly Virginia Couple Safe 200 Miles Away In 19 Minutes
- Minnesota man arrested in Iowa after fatal double shooting charged with murder
- Two Michigan men charged, accused of sexually assaulting woman
- Gwinnett County police seize drugs, more than 30 guns from stolen trailer
- Woman arrested in Kennewick hit-and-run death of Richland mom
- 3 arrested, 4 guns seized after stolen vehicle pursuit through Des Moines Wednesday night
- Lowell woman charged in fatal hit-and-run that killed 72-year-old pedestrian
- Simi Valley doctor and wife gunned down in driveway by their own son, police say
- Suspect linked to 12 ATM break-ins at popular Austin spots, police say
- 1,200-Mile Manhunt Ends In Michigan: 'Dangerous' Pasco County Fugitive Trapped By Traffic Tech
- Columbus police charge man in fatal road rage shooting in Linden
- Portsmouth crime drops 17% in 2025: Police credit data, tech, and community trust
- Rancho Mirage Sees 39% Drop in Property Crime After Boosting Police Presence and Tech
- New revelations on Quincy's FLOCK cameras and homicide numbers
- License plate readers help solve cases quickly in Mo. and Ill.
- Allentown PD reported the fewest homicides since 1989; tech played a role in over 350 investigations.
- Tulsa PD achieved a 100% homicide clearance rate, Flock's LPR technology helped.

You can find attached a letter from NCMEC highlighting why LPRs are important tools for law enforcement in quickly and effectively responding to AMBER Alerts.

We encourage all communities using Flock to develop metrics for success so they can continually assess ALPRs impact on improving their quality of life. We encourage partner agencies to regularly collect data that demonstrates the effectiveness of our technology across key outcomes. Such outcomes include, but are not limited to: arrests by crime type, recovered motor vehicles, recovered property, and located missing persons. Flock is available to assist your agency in developing a data capture strategy. Several agencies collect outcomes data and provide them in a public-facing manner, including Lexington, KY, Mt. Juliet, TN, and Everett, WA.

Accuracy

Flock LPRs have 93% license plate reading accuracy, 95% vehicle color accuracy, 92% vehicle make accuracy, and 98% vehicle type accuracy. Because of Flock's machine learning technology, these rates continue to improve. Third-party tests have shown Flock's technology to be up to 30% more accurate than traditional LPR solutions. Additionally, the cameras self-monitor to ensure connectivity and functionality, and low-confidence plate reads trigger cautionary alerts to the user.

An independent audit by the City of Austin, TX of their Flock LPR program "*found that APD's ALPR program used 4 hotlists, found 13,122 matches, and resulted in 0 incorrect or unjustified stops.*" It additionally found: "*We reviewed each stop justification, compared its rationale to Resolution requirements, and checked with APD for supplementary information where needed. We found zero incidents of incorrect or unjustified stops.*"

Flock Safety confirms both the Optical Character Recognition (OCR)/plate and the state of the plate are both a match before sending a Hot List notification -- this is an extra step that legacy LPR systems do not perform. In side-by-side tests, third parties have found our technology to be up to 30% more accurate than legacy systems.

In the event that a LPR picks up a low confidence plate read, we proactively send an alert to caution the user. We recommend agencies enshrine language resembling the following in their LPR policies: *"Upon receipt of an alert and prior to performing a traffic stop, the law enforcement officer or dispatcher must visually confirm that the scanned plate matches the alert with regard to plate letters, numbers, and issuing state and confirm that the stop meets all applicable law and policies."*

Flock Safety takes accuracy seriously and works diligently to minimize LPR errors. The NCIC database is updated every 12 hours and to ensure the most accurate and up-to-date data, Flock updates its own system every 6 hours. This helps ensure that the information used by Flock's LPR system is as current as possible.

Data Security

Regarding data security and this video specifically, first and foremost, Flock is committed to continuously improving security, has recently pledged to the Secure By Design principles program authored by CISA and continues to engage in regular conversations with CISA as part of our ongoing commitment to these principles.

Flock publicly disclosed many of these findings ourselves in a blog post in May, as well as through the submission to Mitre for inclusion in the National Vulnerability Database. These are not material vulnerabilities, and both severity and likelihood to be exploited are low.

The exploitation of these vulnerabilities require physical access to a device and knowledge of device debugging. If a person was able to gain physical access to the device (which is typically placed on a pole several feet above normal height), they would still not be able to gain access to footage, as the data is only stored for a very limited time duration on the device following its transmission to the cloud. None of these vulnerabilities affect our cloud platform, where the vast majority of all evidence and metadata is stored.

The statement above, "...there is the documented sale of law enforcement Flock Safety accounts, allowing bad actors to purchase access to the entire network of Flock cameras and their databases" is simply false. The device in question in the video was not connected to the cloud and never installed, so the security is akin to factory settings. It's like looking at an iPhone before it is connected to iCloud. Once our devices are connected to the cloud, all our security updates, encryption, and continuous software upgrades are initialized.

Flock secures data in accordance with industry requirements, including encryption using AES-256, as validated by the company's ISO 27001 compliance certification. As our customers have come to expect, Flock continues to prioritize their security by continuously evaluating the security of devices and resolving vulnerabilities in accordance with potential risk to customer environments.

Additional information regarding data security, Flock Safety is designed to provide a comprehensive and secure platform for public safety technology. Our end-to-end data architecture ensures the seamless collection, processing, storage, and analysis of data, including at rest and in-transit, prioritizing security and privacy at every stage.

Flock Safety cameras have no public IP, and therefore, are not addressable remotely to access footage. All data collection points are equipped with secure communication protocols to protect data in transit from interception and tampering. All data is encrypted using industry-standard algorithms (AWS Key Management Service or KMS) before being transmitted to our servers. CJIS data is stored in the AWS GovCloud.

In addition to being certified by the FBI's Criminal Justice Information Services (CJIS), we are NDAA, SOC2 (Type II), SOC3, ISO 27001, Higher Education Community Vendor Assessment Tool (HECVAT), and FERPA-compliant. We are also aligned with the security protocols established by NIST Cybersecurity as well as the Cloud Security Alliance's CAIQ framework.

Additional security precautions include:

- Role-Based Access Controls (RBAC): Ensures users access only the data necessary for their roles.
- Data Encryption: All data is encrypted both in transit and at rest using industry-leading methods.
- Multi-Factor Authentication (MFA): Adds an extra layer of user verification for system access.
- Redundancy and Disaster Recovery: Utilizes AWS's geographically dispersed data

centers to ensure data availability and durability.
- Data Retention and Deletion: Data is automatically deleted after (thirty) 30 days following strict AWS protocols.

A limited configuration issue briefly affected a very small number of Condor video devices, allowing temporary internet access to a troubleshooting-only interface that did not permit camera control, system access, or exposure of sensitive information; no LPR, audio, or trailer devices were impacted. The issue was quickly resolved, affected customers were notified, security updates were deployed, and reports suggesting broader impact are inaccurate. See our blog post on this topic here.

Federal Access/Immigration Enforcement/Reproductive Health

Flock does not presently have a contractual relationship with any U.S. Department of Homeland Security agencies. Flock had engaged in limited pilots with the U.S. Customs and Border Protection (CBP) and Homeland Security Investigations (HSI) which were to assist those agencies with combatting human trafficking and fentanyl distribution.

- The CBP pilot ran 4 months, starting in May 2025 and ending in late August.
- The HSI pilot ran 2 months from March 2025 to May 2025.

Flock remains committed to ensuring that every jurisdiction can use these tools in a way that reflects its local laws and values. Flock continues to reinforce compliance, transparency, and ethical use of technology. We have made policy and product investments to align with evolving state and local laws to include:

Significant investments in compliance and ethical governance:

- Appointed a Chief Legal Officer to lead compliance strategy.
- Tripled Policy-team headcount.
- Expanded Trust & Safety programs.
- Revamped customer training with compliance-specific modules.
- Added a Product Compliance Manager role.
- Released new built-in compliance protections, with more in development.

In addition to the federal agency protocols listed above, we have implemented additional recent product improvements, including:

Search Filters: Immigration and Reproductive Rights

To comply with state laws limiting certain law-enforcement activities, Flock implemented specialized search filters that automatically exclude cameras from searches related to immigration enforcement or reproductive-care investigations.

These filters are active for all searches on the agency's cameras—including shared and statewide/national lookups and are currently applied in states with clear statutory justification.

States with Active Filters:

- Both Filters: CA, CO, IL, NJ, OR, VT, WA
- Reproductive Health Only: CT, HI, ME, MD, MA, NV, NM, NY, DC

All agencies can now choose to automatically exclude their networks from these searches.

We have not heard of a single case where Flock has been used to prosecute someone for reproductive or gender affirming healthcare. While there are conflicting reports about what happened in Johnson County, Texas we took seriously the concerns raised and doubled down on our commitment to ensuring that community safety never has to come at the expense of community values and implemented the comprehensive search filter noted above.

Federal Agency Protocol

Moving forward, federal agencies on Flock are treated separately to protect privacy and meet state requirements:

- Excluded from Statewide & National Lookup.
- Excluded from auto-approved sharing requests.
- Clearly tagged in the user interface.
- Bound by additional restrictions in states such as CA and VA.

Data Access/Ownership/Sharing/Audit Capabilities

Your city owns your data and is in complete control of who can access your system and under what conditions you will share your data with other law enforcement agencies, so it aligns with your values. Flock Safety will never sell your data. Flock will never share your data without your permission, unless legally required to do so.

Only the authorized users your community designates will have access to your system, and even then every search they make must have a reason in order to do a search. Every search made by one of your authorized users is logged and able to be audited so you can see when and how your system is being used. Flock recommends every community perform regular audits to ensure compliance with your community's laws and regulations. Flock also has additional improvements and tools coming soon that will give agencies greater control, auditing power, and trust in shared data to include:

Granular Sharing Controls

Administrators will soon be able to:

- Define which permission types can be requested per network.
- Eliminate unnecessary or irrelevant requests (e.g., for restricted areas).
- Lay groundwork for regional or radius-based rules.

Organization-Level Search Filters

Agencies can now self-enroll in immigration or reproductive-rights filters within Organization Settings.

- Visibility into which team member activated the filter.
- Clear confirmation of active compliance status.

Standardized Search Reasons

Soon the open-text “Search Reason” field will shift to dropdown Offense Type categories based on NIBRS data and customer feedback.
Benefits:

- Prevents vague or unacceptable entries.
- Enables stronger enforcement of filters.
- Improves analytics and case-closure accuracy.

Proactive Auditing & Anomaly Detection

Flock is developing intelligent auditing to surface potential misuse automatically.
Focus areas:

- Searches possibly unrelated to crimes.
- Excessive or repeated searches.
- Off-hours activity.

[WPD: We are happy to discuss further with your elected officials, if needed. Please let us know if you have questions.]