

Public Safety Committee Packet

Review of Flock Safety Automated License Plate Reader (ALPR) Program

Discussion of Safeguards, Transparency, and Continued Use

Prepared by: Anthony W. Carlson Public Safety Chair

Purpose: Review current Flock Safety safeguards, discuss public concerns, evaluate additional departmental safeguards, and consider recommendations regarding continued use of the system.

Meeting Objective

The purpose of this discussion is not to determine whether technology should exist, nor to presume misconduct has occurred.

The purpose is to evaluate:

- The value the Flock system provides to our Police Department.
 - Existing safeguards within the Flock platform,
 - Additional safeguards that may be appropriate at the department level.
 - Opportunities to increase transparency and public confidence.
 - Whether continued use should be accompanied by additional policy guidance.
-

Opening Statement

As Public Safety Chair, I believe our responsibility is to provide all of our public safety professionals with the most effective tools possible, while ensuring those tools are used responsibly, transparently, and in a manner that respects the rights of our residents.

Technology such as Flock has proven to be a very valuable investigative resource. However, the effectiveness of any tool must be matched equally by appropriate safeguards. Policies, oversight, accountability, and public transparency must be in place and upheld.

My concern is not whether the technology should exist. My concern is whether we have established sufficient safeguards to ensure it is used consistently, appropriately, and in a way that maintains public confidence.

When residents know that strong oversight exists, and when our law enforcement professionals can clearly demonstrate responsible use, both public safety and public trust are strengthened.

Our goal should be neither unrestricted use nor unnecessary restriction. Our goal should be responsible governance that supports public safety while protecting the community we serve.

I recognize that the Flock system provides significant value to law enforcement investigations and public safety efforts. I also recognize that no technology is immune from misuse because no system can completely overcome human nature.

The recent safeguards implemented by Flock, including reduced data retention periods, required case numbers for searches, automated auditing tools, access controls, and enhanced security measures, appear to be meaningful improvements that reduce opportunities for abuse.

However, technology safeguards alone are not enough. Effective governance requires clear departmental policies, periodic review, accountability for misuse, and transparency with the public regarding how these tools are governed.

I believe government exists to protect the rights and liberties of its citizens. As such, government should be self-limiting rather than self-expanding. When powerful tools are entrusted to government agencies, it is appropriate that equally strong safeguards accompany them.

My interest is not in removing effective tools from the hands of public safety professionals. My interest is in ensuring that the use of those tools is governed responsibly and appropriately, and supported by policies that maintain public trust while protecting individual rights.

Public Comment Opportunity

Chair Statement

Before committee discussion begins, I would like to provide an opportunity for public comment.

We recognize that automated license plate reader technology generates strong opinions from both supporters and opponents. We welcome and value respectful observations, concerns, questions, and recommendations from residents.

The purpose of this discussion is to better understand the benefits, risks, and safeguards associated with this technology and determine whether additional policy measures should be considered.

Comments should be directed to the committee and limited to the operation, oversight, transparency, and governance of the system. In the necessity of time we must enforce a 3 minute time limit.

Currently Implemented Flock System Safeguards

Data Retention and Evidence

Reduction to Seven-Day Data Retention

- Default retention reduced from 30 days to 7 days.
- Data automatically expires unless preserved for an active investigation.

Evidence Mode

- Data may only be retained beyond seven days when connected to an active criminal investigation.
-

Access and Misuse Controls

Mandatory Audit Assistance

- Automated monitoring identifies unusual search behavior.

- Audit tools are now standard.

Automatic Lockouts

- Users engaging in abnormal search activity can be automatically suspended pending review.

Required Case Numbers

- Searches require a valid case number or documented reason.
 - Exceptions are limited to verified emergencies such as missing children.
-

System Security

Multi-Factor Authentication (MFA)

- Required for all users.

Independent Security Review

- Third-party review of system security.

Coordinated Vulnerability Disclosure

- Formal process for reporting and correcting vulnerabilities.
-

Key Discussion Principle

People often fear what they do not understand, and they mistrust what they cannot see.

The purpose of safeguards should therefore be two-fold:

1. Prevent or detect misuse.
2. Demonstrate to the public that misuse is being prevented and monitored.

A department may have excellent controls in place, but if residents are unaware of those controls, public confidence may remain low.

Transparency and accountability help close that gap.

Considerations Regarding Implementation

The purpose of the recommendations contained in this packet is not to interfere with criminal investigations, direct day-to-day police operations, or restrict lawful investigative discretion.

Rather, the purpose is to establish reasonable governance, accountability, transparency, and oversight measures that support public confidence while preserving the effectiveness of the Flock system.

The Committee recognizes that Flock Safety has implemented significant platform-level safeguards, including reduced retention periods, required case numbers, audit tools, access controls, misuse detection mechanisms, and enhanced security protections. The recommendations discussed herein are intended to complement, rather than replace, those existing safeguards.

The Committee further recognizes that operational procedures are best developed by law enforcement professionals. While the Committee may establish policy expectations and governance objectives, the specific methods of implementation should remain subject to departmental procedures, applicable law, operational considerations, and professional judgment.

At the same time, the Committee recognizes that automated license plate reader technology is a powerful investigative tool. Continued public confidence requires not only effective technology safeguards, but also clearly communicated local policies, accountability measures, and transparency regarding how the system is governed.

Should the City elect to continue utilizing the Flock system, it is reasonable to expect that meaningful safeguards, training requirements, audit procedures, and transparency measures accompany that decision.

Department-Level Safeguards for Consideration

1. Written Authorized Use Policy

Develop and publish a formal policy defining:

- Authorized users.

- Authorized purposes.
- Prohibited uses.
- Search documentation requirements.
- Audit procedures.
- Supervisory responsibilities.
- Consequences for misuse.

Example Language

Use of the system for personal, political, commercial, or non-law-enforcement purposes is strictly prohibited.

2. Establish a supervisory review process for system activity.

Suggested Policy Requirement

The Department shall incorporate supervisory review of system activity into departmental policy. The specific frequency, scope, sampling methodology, and documentation process may be determined by the Department based upon operational needs, available resources, and evolving best practices.

Benefits

- Human oversight.
 - Accountability.
 - Policy compliance verification.
-

3. Annual Policy Review

Technology changes rapidly.

Policies should evolve as well.

Suggested Policy Requirement

The Department shall periodically review ALPR-related policies and procedures and recommend revisions as necessary to maintain consistency with legal requirements, operational needs, technological developments, and established best practices.

4. User Training

Prior to system access, users should complete:

- Initial system training.
- Privacy training.
- Policy review.
- Periodic refresher training.

The Department shall establish training requirements consistent with operational needs and applicable policy requirements.

5. Misuse Review Process

Establish a documented process for:

- Reporting potential misuse.
- Reviewing allegations.
- Restricting or suspending access when appropriate.
- Corrective action consistent with applicable personnel policies.
- Documentation and record retention.

Clarification

The purpose of this recommendation is not to involve the Committee in personnel matters, disciplinary decisions, or internal investigations. Rather, the purpose is to ensure that an appropriate review process exists and is consistently applied.

Transparency Measures

1. Publish the Policy

Make policies available through:

- City website.
- Public records portal.
- City newsletter.
- Social media announcements.

Residents should not need to submit an open records request merely to understand the rules governing the system.

2. Quarterly Transparency Report

Potential reporting categories:

- Number of cameras deployed.
- Number of searches conducted.
- Number of investigations assisted.
- Number of evidence preservation requests.
- Number of audits completed.
- Number of misuse complaints received.
- Number of misuse incidents substantiated.

No investigative details would be disclosed.

Aggregate reporting provides accountability while protecting investigations.

3. Quarterly Public Safety Committee Review

Request periodic updates from the Chief regarding:

- Utilization statistics.
 - Audit findings.
 - Complaints received.
 - Policy compliance.
 - Policy recommendations.
 - Effectiveness of newly implemented safeguards.
-

4. Citizen Complaint Process

Provide clear guidance regarding:

- How concerns may be submitted.
- Who receives complaints.
- How complaints are reviewed.

- How outcomes are documented.

Even infrequently used processes contribute to public trust.

5. Public Education Initiative

Develop a simple fact sheet explaining:

What the System Does

- Captures license plate information.
- Assists criminal investigations.
- Helps locate stolen vehicles.
- Assists in locating missing persons.

What the System Does Not Do

- Capture the identities of drivers.
- Record conversations.
- Conduct facial recognition.

Safeguards

- Seven-day retention limit.
- Required case numbers.
- Automated auditing.
- Automatic misuse detection.
- MFA protection.
- Supervisory oversight.

When people understand the system, rumor loses power.

Guiding Principle

Transparency is not about proving the department is untrustworthy. Transparency is about proving to the public that trust is warranted.

Recommendations for Consideration

The committee may determine that continued use is appropriate with additional safeguards, determine that further review is necessary, or determine that continued use is not warranted.

Suggested Safeguards for Consideration

1. Adoption of a formal written use policy.
2. Mandatory user training and annual refreshers.
3. Supervisory audit requirements.
4. A documented misuse review process.
5. Public-facing publication of governing policies.
6. Quarterly Public Safety Committee review.
7. Quarterly public transparency reporting.
8. Annual policy review and update.

Possible Recommendation:

The committee may recommend continued use of the Flock system provided that formal policies, audit requirements, transparency measures, training requirements, and ongoing oversight mechanisms are implemented and maintained.

Closing Statement

Government should be powerful enough to perform its legitimate duties, but restrained enough to protect the liberties of the people it serves.

The question before us is not whether technology should be available to law enforcement. The question is whether that technology is governed in a manner consistent with public trust, individual rights, accountability, and transparency.

If we choose to utilize powerful tools, we have an equal responsibility to implement meaningful safeguards. By combining policy, oversight, and transparency, we can equip our public safety professionals with the tools they need, while maintaining the confidence of the community they serve.

Flock Question and Answer

Flock violates the Fourth Amendment

The Fourth Amendment protects places (think trespassing) and people (think individual privacy) from unreasonable searches and seizures.

The Fourth Amendment states, “The right of the people to be secure in their persons, houses, papers, and effects, against **unreasonable searches and seizures**, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

Katz v. United States (1967) is a key case to defining a search that triggers a warrant or warrant exception. In the case, federal agents attached an electronic listening device to the outside of a public phone booth used by Charles Katz. Katz was a bookie involved in interstate gambling. Even though the device never entered the booth, the Supreme Court held the government had violated Katz’s reasonable expectation of privacy, and therefore conducted a search under the Fourth Amendment. The decision rejected the older “trespass” rule and created the modern privacy-based standard: what a person seeks to keep private, even in a public space, may be constitutionally protected.

Based on Katz, a “search” occurs when:

1. An individual actually expects privacy, and
2. Society recognizes that expectation as reasonable.

United States v. Jones (2012) is a foundational case defining how the Supreme Court views GPS tracking of vehicles. In Jones, the Court held that law enforcement’s warrantless installation of a GPS tracking device on Antoine Jones’s vehicle—and its use to monitor his movements for 28 days while investigating him for drug trafficking—constituted a Fourth Amendment search. Before Jones, officers relied on *United States v. Knotts* (1983), where the Court upheld the warrantless use of a radio “beeper” hidden in a chloroform container purchased by defendant Leroy Knotts, who was suspected of manufacturing drugs. In Knotts, the Court concluded there was no Fourth Amendment violation because individuals have no reasonable expectation of privacy in their movements on public roads. Jones, however, changed the legal landscape by holding that physically attaching a GPS device to a vehicle—an “effect” protected by the Fourth Amendment—was a trespass undertaken to obtain information, making it a per se search regardless of any privacy expectation in public travel. The decision revived the Amendment’s property-based (trespass) roots while also recognizing that modern, long-term electronic monitoring raises privacy concerns under the Katz reasonable-expectation-of-privacy standard.

Carpenter v. United States (2018) is a key case to gaining insight into cell-site location data. In *Carpenter v. United States*, the Supreme Court held that police must obtain a warrant before accessing a person’s historical cell-site location information (CSLI), rejecting the government’s use of lower-standard court orders to collect 127 days of Timothy Carpenter’s location data during a robbery investigation. The Court reasoned that CSLI creates a deeply revealing, long-term record of a person’s movements, and because cell phones automatically generate this

data without meaningful user choice, individuals retain a reasonable expectation of privacy in it. By treating the government's acquisition of this information as a Fourth Amendment search, the Court limited the traditional third-party doctrine and signaled that modern, pervasive digital tracking requires stronger constitutional safeguards.

Chatrue v. United States (2026) is a key case in understanding geofence warrants and developing a suspect through mobile application location history data. The Supreme Court addressed whether a “geofence warrant”—a multi-step subpoena directed at Google for users’ Location History data within a specified time and place—constituted a Fourth Amendment search. Police, investigating a bank robbery in Virginia, obtained a warrant requiring Google to produce anonymized data for devices in a 150-meter radius of the scene before and after the crime, gradually narrowing to identify suspects. The Court held that retrieving this intensely detailed location history without a conventional warrant was indeed a search, because individuals maintain a reasonable expectation of privacy in their location history—even if it’s held by third-party tech companies. The decision extended *Carpenter’s* reasoning, noting Location History is even more precise and personally controlled, isn’t voluntarily shared in a meaningful sense, and can chronicle everything from public movements to private stops. The Supreme Court remanded questions about the warrant’s specificity and probable cause to the lower courts but firmly established that accessing this data implicates Fourth Amendment protections. Bottom-line: acquiring device-location data from a company is unquestionably a Fourth Amendment search and must be done pursuant to a warrant, but Chatrue leaves open whether even a warrant is sufficient—particularly when such warrants inevitably sweep up data from innocent bystanders. The unresolved question is whether the current three-step Google process satisfies constitutional standards or whether something more robust is required to overcome the privacy interests implicated by dragnet-style location searches. It may ultimately be that only circumstances like national-security threats or true life-and-limb exigencies can justify warrants that collect sensitive data on non-suspects caught within the geofence.

The Supreme Court has made clear that continuous **GPS tracking**, whether via a device physically attached to a vehicle (*United States v. Jones*, 2012), or embedded in a cell phone, is a search under the Fourth Amendment and therefore requires a warrant because it involves physical trespass or invasive monitoring. Likewise, **Google Location History**, which compiles a high-precision, multi-source log of a device’s movements (using GPS, Wi-Fi, cell towers, Bluetooth, etc.) at intervals as brief as two minutes and within tight spatial bounds (~20 m), also constitutes a search when accessed by law enforcement via geofence warrants (*Chatrue v. United States*, 2026). Finally, historical **cell-site location information** (CSLI)—data from which a phone’s approximate location is inferred via cell towers—has been ruled a search requiring a warrant in *Carpenter v. United States*, 2018, because it reveals an individual’s comprehensive movements over an extended period. Together, these cases demonstrate that as location-tracking technologies grow more detailed and precise, the Court consistently demands warrant protection to uphold privacy rights.

Based on judicial precedent, here is what courts consider when deciding whether a Fourth Amendment search exists:

1. **Continuous or aggregated tracking:** Does the technology allow law enforcement to follow a person’s movements over time—creating a continuous or retrospective record rather than a single, momentary observation?

2. **Revealing private life:** Does the data expose personal, sensitive patterns—such as where a person worships, works, socializes, seeks medical care, or spends the night—that go beyond what could be learned from ordinary public surveillance?

But what about ALPR? Does the warrant requirement for GPS → Google Location History → Cell-Site Location Information → also extend to Flock Safety cameras?

In **Schmidt v. City of Norfolk (2026)**, residents Lee Schmidt and Crystal Arrington challenged Norfolk’s deployment of approximately 170 Flock Safety ALPR cameras under § 1983, arguing that the city-wide system enabled warrantless, dragnet-style tracking of their vehicle movements—recording over 500 sightings combined in only four months—and thus violated their Fourth Amendment rights. The court granted summary judgment in favor of the City, concluding that the camera network did not amount to a constitutional search because it only captured brief, intermittent plate readings on public roads and did not reconstruct the “whole of a person’s movements” akin to extended cell-phone tracking under *Carpenter*. The judge emphasized that ALPR data collection as currently deployed—without continuous, real-time surveillance or deep retention—does not intrude on a reasonable expectation of privacy. He also warned that the conclusion might change if the system becomes more pervasive or data retention increases. This case is currently under appeal.

Here is a side-by-side comparison of Norfolk and Nekoosa:

	Norfolk	Nekoosa
# of Cameras	176	6
# of Camera Clusters	75	0
Area (square miles)	66 square miles	3.4 square miles
Cameras/Square Mile	2.7	1.8
Clusters/Square Mile	1.1	0
Roadway (length in miles)	1,700 miles	20.4 miles
Cameras per Mile	0.10	0.30
Clusters per Mile	0.04	0
Retention Period	21 days	30 days
Locations	Major corridors and primary entry and exit points, with the goal of capturing vehicle movement along key routes where criminal activity is most likely to transit.	3 cameras along major corridors and primary entry and exit points, with the goal of capturing vehicle movement along key routes where criminal activity is most likely to transit. 3 cameras to capture potential and active threats to schools.

Schmidt v. City of Norfolk is not binding on Wisconsin but is instructive. Should a court analyze the City of Nekoosa on similar facts and apply similar reasoning, it would likely rule in our favor. Based on a side-by-side comparison, the concentration of cameras in Nekoosa is less than Norfolk.

The following outlines how Flock ALPR is meaningfully different than other technologies that trigger Fourth Amendment protections:

No continuous or comprehensive tracking:

ALPR cameras capture isolated snapshots of a license plate at a point in time, not a device's continuous movement. They do not follow a vehicle everywhere or generate a persistent timeline of travel the way GPS, CSLI, or Google Location History do.

No automatic creation of a movement log:

ALPR systems record only the moment a vehicle passes a camera. They do not automatically chart routes, infer destinations, or create a minute-by-minute movement map comparable to Google's Location History or CSLI databases.

Public exposure, not private intrusion:

License plates are already exposed to anyone on public roads. ALPR tech captures only information already visible—unlike GPS devices (which are physically attached) or Location History (which logs private, sensitive stops such as homes, workplaces, churches, medical providers).

Gaps in coverage prevent “whole-movement” surveillance:

ALPR networks—even large ones—contain physical gaps. They cannot replicate the seamless, high-frequency, 24/7 geolocation tracking seen in GPS or Google Location History.

Does not reveal intimate details of private life:

ALPR cannot determine who was driving, why they went somewhere, how long they stayed, or where they walked once parked. It does not show entry into private areas (homes, medical offices, religious institutions), which was central to the Court's reasoning in *Carpenter* and *Chatrie*.

Short retention periods limit aggregation into meaningful patterns:

Systems like Norfolk's (21-day retention) and Nekoosa's (30-day retention) store only short, fragmented data sets—far less revealing than months-long CSLI or Google Location History archives.

No trespass or “device attachment”:

Unlike *Jones*, ALPR involves no physical intrusion on a vehicle or personal property. There is no “trespass-based” search element.

Flock cameras continuously track people

The ALPR system does not continuously track individuals. It captures only license plates and basic vehicle characteristics as vehicles pass fixed cameras positioned on major corridors and primary entry and exit routes. The majority of Nekoosa's city streets has no ALPR monitoring at all. The system is built to detect vehicle movement through key travel routes—not to follow specific people, map daily routines, or monitor residential neighborhoods.

Nekoosa has no camera “clusters.” Each camera is one-directional and generally captures one-way traffic. Camera clusters are mounted to monitor traffic going both ways.

Benjamin Franklin says, “Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety.”

This quote is often taken to mean that any trade-off between liberty and safety is unacceptable. But that’s not what Franklin was arguing.

Franklin’s warning is important, but historically he was not opposing reasonable public-safety measures. He was saying that emergencies don’t give government permission to surrender *essential* liberties.

In 1755, during the French and Indian War, Franklin, as part of the Pennsylvania Assembly, used this language in a dispute with Governor Robert Morris. The frontier was under attack, and the governor wanted to raise funds to strengthen defenses. The Assembly agreed and allocated £60,000—more than enough for defense. The disagreement wasn’t about whether to defend the colony; it was about **who should pay**. The governor insisted the Penn family, who owned the colony, should be exempt from taxation. The Assembly argued that exempting them was unfair and violated the legislature’s authority. They passed a bill asking the King to resolve the issue, but the governor rejected it.

So Franklin’s statement wasn’t a rejection of government taking reasonable actions to protect people. It was a rejection of abandoning essential liberties—like fair representation and taxation—under the pretext of crisis.

Our current discussion isn’t about who funds ALPR; it’s about whether ALPR is a **reasonable** tool.

Let me just point out that ALPR doesn’t give police a new power to observe vehicles in public. It provides a more efficient, searchable way to document what officers can already observe manually. Instead of requiring officers to:

- canvas neighborhoods
- watch hours of video
- manually read plates
- contact neighboring agencies
- circulate BOLOs
- or wait for an officer to encounter a suspect vehicle

ALPR offers an investigative lead. And importantly: An ALPR hit is **not** probable cause. A responsible agency, like ours, requires officers to independently verify the information before taking enforcement action.

In short, Franklin believed government has a duty to protect its people using reasonable measures. The real question for us is whether ALPR is one of those measures—and whether we use it responsibly.

Officers across the state and nation are misusing the technology

Yes—some officers have misused ALPR technology. In Wisconsin, four officers have been arrested and charged for improper use.

But it's important to keep perspective: that's four out of roughly 13,000 officers statewide. Media coverage can make the problem feel widespread, but the actual number of offenders is very small.

If we eliminated every technology that has ever been misused by an officer, we'd have very little technology left. Misuse doesn't stem from the tool itself—it stems from the individual using it.

Technology acts as an amplifier of character. It makes the intentions of the user more visible. When someone is committed to serving ethically, technology helps them do good work. When someone has ill intent, technology can expose that behavior quickly.

Our department has long emphasized hiring for character and training for skill. We look for good people first. But even good people sometimes make bad decisions, and occasionally someone who shouldn't wear the badge slips through.

The good news is that ALPR systems like Flock include strong accountability features. Officers who misuse ALPR are often misusing other systems too, and ALPR helps us identify those individuals. Rather than enabling misconduct, this technology actually helps us detect and address it—ensuring the integrity of our agency and improving public trust.

Other communities in Wisconsin are non-renewing or ending contracts with Flock for things like contract violations, unauthorized data disclosures, and misrepresentation of system capabilities (i.e., encryption). Why doesn't Nekoosa share those same concerns?

It's important to acknowledge a few realities.

Flock Safety is still a relatively young company. In about nine years, they've grown rapidly and become the national leader in fixed ALPR systems. Any company that expands that quickly will experience growing pains. Just like a child learning to walk, there will be missteps along the way—none of which are surprising or unique to Flock.

There has also been significant political, media, and community scrutiny directed at Flock. When any single company receives that level of attention, flaws will inevitably be found. Intense inspection uncovers areas for improvement in every organization.

We can't speak for decisions made by other agencies, because each community has its own expectations, policies, experiences, and contracts. What we can speak to is our relationship with Flock Safety and what we've seen firsthand.

The Flock team members we interact with have been professional, responsive, and genuinely committed to delivering a reliable product that supports public safety. When concerns have been raised, they have engaged with them constructively and made continuous improvements. Based on our experience, we have not identified contract violations or misconduct that would justify terminating our five-year agreement.

In short, Nekoosa's position isn't that problems elsewhere don't matter. It's that our direct experience, oversight, and contract performance have not reflected the issues some other communities have reported. We monitor the partnership closely, and at this time, we have confidence in the company's accountability, responsiveness, and commitment to improving the technology.

We've heard that in some places, like Sheboygan, that Flock is selling data. Isn't that a violation of the contract?

We can't speak to Sheboygan's contract or their interpretation of it. Every municipality negotiates its own terms, and we're not in a position to comment on how another city manages its agreement.

What we *can* speak to is our own contract with Flock Safety. Our agreement allows Flock to use anonymized data for machine-learning purposes—primarily to improve the technology—and for optional products such as Traffic Analytics. This is an area where communication from Flock could have been clearer. We did not know they offered a Traffic Analytics product until we saw it reported in the news, nor were we initially aware that anonymized data was being retained longer than our standard 30-day period.

Once we learned this, we contacted our Flock representative and here's what we confirmed:

- Traffic Analytics provides information like traffic volume, speed trends, and roadway patterns to support transportation planning.
- To generate this, Flock strips all identifiable information—images, license plates, and any link to a specific vehicle—leaving only fully anonymized data.
- Flock may retain this anonymized data for up to five years to support those analytics.
- The data still belongs to the City of Nekoosa.
- Flock may offer additional services using our data, at an additional cost, but they cannot sell that data to third parties. This is explicitly prohibited by contract.
- Our understanding of what occurred in Sheboygan is that Flock attempted to sell *a product* built on that city's data—not the data itself. If Flock offered us a similar add-on product, they would be within the rights outlined in our contract.

This kind of optional add-on is not unusual. Many technology vendors offer toggle-based features that agencies can opt into or out of depending on need and budget. Whether we adopt an add-on depends on whether it provides sufficient value for its cost.

In short, based on our contract and our direct communication with Flock, we have no evidence that they are selling our data or violating the terms of our agreement.

What about concerns over unauthorized data disclosures?

The incidents that have upset some agencies stem largely from how different communities and states handle open-records laws. FOIA requests have increased significantly due to heightened media interest, and each state has its own requirements for what must be released.

In December, we learned that some agencies around the country provided unredacted Network Audit logs in response to FOIA requests. For context, when an officer conducts a search using the nationwide option, details such as a license plate or case information appear in that log. The decision to release those logs was not made by Flock—it was made by the agencies responding to the FOIA requests. Unfortunately, once released, these logs were posted on a public website that allowed anyone to search their own plate—or someone else’s—to see whether law enforcement had queried it.

While we have no evidence that any of our investigations were compromised, it’s easy to see how such disclosures could harm ongoing cases or lead the public to draw incorrect and damaging conclusions.

To protect the integrity of our data and investigations, we disabled nationwide search and sharing in August of this year. Almost all of our investigative needs are met by our own cameras or those within Wisconsin, so this change was operationally sound and significantly reduced exposure.

Flock also took action. They changed the way Network Audit records are generated so that they now come partially redacted, reducing the risk of sensitive information being released. If someone wants a fully detailed log, they would need to contact individual agencies directly and request an Organizational Audit—the internal tool agencies use to monitor their own personnel.

In short, the unauthorized disclosures were not caused by Flock violating the contract. They were caused by agencies releasing unredacted information under their respective open-records laws. We responded and Flock adjusted its practices to further reduce risk. Together, those steps ensure we maintain greater control over our data and protect the integrity of our investigations.

What about concerns over data security?

We understand the concerns—many of us have seen the same videos, podcasts, and articles raising questions about ALPR data security. Here’s what we can say with confidence about our system.

Only trained and authorized personnel can access ALPR data. Every user has an individually assigned account secured with multi-factor authentication, and supervisors actively monitor permissions, usage, and audit logs to ensure the system is being used appropriately.

Before the data ever reaches us, Flock Safety applies multiple layers of security. They use strong encryption, rely on independent third-party security auditing firms, and publicly disclose vulnerabilities along with the fixes they implement. Their published responses show they investigate security findings, register them with national databases, and issue hardware or software updates when needed. In other words, they treat vulnerabilities seriously and address them transparently.

And as of today, unlike some communities across the country, we have not faced attempts to criminally compromise or “hack” our ALPR cameras. We remain vigilant, and we continually review new information, but based on our experience and the safeguards in place, we have confidence in the security measures protecting our data.

A local media source has reported that the City may be able to exit its contract early without penalty. Is that true?

No. As we’ve consistently shared, our current contract—which runs through 2028—cannot be terminated simply because the City chooses to end it. Unless there is a material breach by the vendor that cannot be corrected, we are obligated to the full five-year term. If the City ended the agreement early for any reason other than a legitimate breach, we would have paid in advance for a service we no longer utilize.

The recent media report suggested the City could exit the contract using the non-appropriation clause found at the end of the agreement. While non-appropriation clauses do exist to address true, documented financial hardship, they are not designed as a tool to end contracts for policy or preference reasons. Invoking non-appropriation without clear evidence that the City is genuinely unable to pay would carry significant legal risk. Doing so could reasonably be interpreted as an improper use of the clause, opening the door to breach-of-contract litigation.

In short, the contract cannot be terminated for convenience, and using non-appropriation as a workaround would not be legally defensible without verified financial necessity.