Written Testimony for Agenda item 2: Member discussion on ALPR and Body Camera reporting requirements

December 10th, 2025
Samuel Chapin
Hastings, Minnesota

Non-compliance with statute 13.824 subd. 8 (Notification to Bureau of Criminal Apprehension)

I have personally witnessed one case where a law enforcement agency has entered into a contract with a company offering ALPR services and devices to the agency, where the agency does was non-compliant in sending their list of erected ALPRs to the Bureau of Criminal Apprehension for several months. I suspect there are a number of other agencies whom are not in compliance with this subdivision, and am in the process of submitting MGDPA requests for many other jurisdictions in order to better understand the severity of the issue.

Timeline of events:

- **12/16/2024**: The Elk River Police Department signed a contract with Flock Safety for *15* Flock Safety Falcon ALPR devices[1].
- **6/24/2025**: The Elk River Police Department erected an ALPR device near the intersection of Jackson Street and Holt Street in Elk River, Minnesota[2].
- **11/5/2025**: I contacted the Elk River Police Department via email, asking for the date in which said ALPR device was erected as I had not seen the device on the Bureau of Criminal Apprehension website as legally mandated[3].
- **11/7/2025**: I received a reply via email containing the date of erection of said device[3].
- **11/12/2025**: The Elk River Police Department sent a list of their ALPRs to the Bureau of Criminal Apprehension for *17* ALPR devices (two more than the contract had stated)[2].
- **11/17/2025**: I submitted a MGDPA request to The Elk River Police Department primarily for their ALPR contract and communications between the agency and the Bureau of Criminal Apprehension[4].

Within the document I received as part of my MGDPA request, I received a policy manual which includes the text "The Bureau of Criminal Apprehension shall be notified within 10 days of any installation or use and of any fixed location of an ALPR."[5]. I cannot say for certain if this was intentional or negligence on their part, but they should have known to submit the list of ALPRs long before being contacted about it.

An anonymous member of my community had a very similar interaction with the University of Minnesota Police Department[6], more on the UMPD at the end of this document.

1: https://github.com/SChapin97/Minnesota-ALPR-Documentation/blob/164e5085e22c60c80ac0af1e8242803b52ccd920/public_records_documents/dpa_documents/city_police_departments/elk_river_police_department/elk_river_flock_contract.pdf

2:
https://github.com/SChapin97/Minnesota-ALPR-Documentation/blob/164e5085e22c60c80ac0af1e8242803b52ccd920/public_records_documents/dpa_documents/city_police_departments/elk_river_police_department/elk_river_alpr_list_for_bca.pdf
3:
https://github.com/SChapin97/Minnesota-ALPR-Documentation/blob/9ef0bb57d6c3e11e4b1c63169d97aad110828c92/public_letters/letters_to_congress/resources/redacted_elk_river_alpr_location_question.pdf
4:
https://github.com/SChapin97/Minnesota-ALPR-Documentation/blob/74fca092e0c4ee32de3793686f75c37ef3f10a77/public_letters/letters_to_congress/resources/elk_river_dpa_request_email.pdf
5:
https://github.com/SChapin97/Minnesota-ALPR-Documentation/blob/9ef0bb57d6c3e11e4b1c63169d97aad110828c92/public_records_documents/dpa_documents/city_police_departments/elk_river_police_department/elk_river_alpr_policy_manual.pdf
6:
https://github.com/SChapin97/Minnesota-ALPR-Documentation/blob/164e5085e22c60c80ac0af1e8242803b52ccd920/public_letters/letters_to_congress/resources/umpd_flock_rich_text.pdf

Cybersecurity issues

This section is mainly on ALPR devices and software from Flock Safety, as they are the most common stationary ALPRs and have the most amount of independent testing on their products.

In November of 2025, Journalist Benn Jordan uploaded a video titled “We Hacked Flock Safety Cameras in under 30 seconds” to YouTube[1] wherein he brings the following issues to light. Each bullet point starts with a timestamp for the video linked at the end of this page.

- (4:22) The camera can be turned into a debug mode (signified by a blue light) which enables trivial wireless access to the camera’s software. This debug mode can be entered with **a simple combination of button presses**.
- (5:30) There are exposed USB ports where an adversary can plug in a simple, **$6 device** that acts like a keyboard and can **gain full (and remote) access to the device within seconds**.
- (6:25) The software is running in debug mode, which allows an adversary to easily modify or execute malicious code on the device. This means **an adversary can not only overwrite data, but also wipe any trace of their software intrusion (thus making it impossible to tell real versus doctored ALPR data)**.
- (11:45) **Flock cameras take photos when *any* movement is detected, not just when a license plate is detected**. This can include non-vehicle data such as pedestrians crossing the street (which would **run afoul of 13.824 subd. 2(a)**). Additionally, all images stored on device are **entirely unencrypted**.
- (14:10) In a segment on an unsecured Flock Safety API for their nationwide surveillance network (more on that in the next section of this document), they zoom out onto a map of the United States where it is clear that **at minimum 2 Flock Safety devices in the state of Minnesota were accessible on the nationwide network** (which has been known to be used by the Customs and Border Patrol agency without the permission from the law enforcement agency that owns the data[2]).
- (18:45) Flock Safety ALPR devices are running Android 8.1.0 (**which has not received any security updates since 2021** and has many top severity vulnerabilities -- 64 10.0 CVSS vulnerabilities by my count[3]). In conjunction with having negligible physical security, this is a recipe for disaster when it comes to the security and integrity of non-public vehicle and license plate data.

Other areas of concern:

- 404media reporting that the Customs and Border Patrol agency had been accessing ALPR data in Colorado (and other states) without getting direct consent from the law enforcement agency who owns said data.[2]

1: https://www.youtube.com/watch?v=Pp9MwZkHiMQ
2: https://www.9news.com/article/news/local/flock-federal-immigration-agents-access-tracking-data/73-a8aee742-56d4-4a57-b5bb-0373286dfef8
3: https://www.cvedetails.com/version/565966/Google-Android-8.1.html

Consumer privacy issues and concerns

I will again be referring to Flock Safety devices for this section as the main point of contention as their business practices are the most well documented.

In every contract that an entity signs with Flock Safety, they must agree to their terms and service, which is typically represented by a link to their terms and conditions on their website[1] (and are not given a copy of the current terms so it's very easy for conditions to be changed after the terms have been agreed upon – in fact the popular archival site web.archive.org is not allowed to archive snapshots of this site[2] so it's entirely unknown to the public what items Flock Safety has changed in their terms of service over a period of time).

In Flock Safety's terms and conditions, the Customer (in this case, a law enforcement agency) is given full and total control of the data generated from the ALPR devices they lease from the company (4.1 Customer Data and 4.2 Customer Generated Data). The very next condition states that **Flock is given a worldwide and perpetual license for using said data owned by the customer for use as training data in order to improve machine learning algorithms** (4.3 Training Data). On December 1st, 2025, 404Media (in conjunction with Wired) reported on an exposed online panel which Flock uses to coordinate with workers who annotate audio and visual data in order to better improve its machine learning algorithms[3]. **At least some of these workers are stationed in the Philippines**, which raises immense concern for data safety and privacy for Minnesotan and American citizens, especially as condition 11.10 (Export) states that data must not be exported outside of the United States due to regulatory issues.

1: https://www.flocksafety.com/legal/terms-and-conditions
2: https://web.archive.org/web/20250000000000*/https://www.flocksafety.com/legal/terms-and-conditions
3: https://www.wired.com/story/flock-uses-overseas-gig-workers-to-build-its-surveillance-ai/?ref=404media.co

Legal precedence that mass adoption of ALPRs may constitute a Fourth Amendment crisis

In *Katz v. United States (1967)*, it was decided by the Supreme Court of the United States that the Fourth Amendment rights to "be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" applies not only to a person's property, but **the Fourth Amendment also protects a person's "reasonable expectation of privacy"**. In *United States v. Jones (2012)*, SCOTUS decided that the placement of a GPS tracker on a person's car is trespassing on their property and constitutes a search under the Fourth Amendment. In her concurring opinion on this case, Justice Sonia Sotomayor cites *Kyllo v. United States (2001)*, writing "*Rather, even in the absence of a trespass, '**a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.**'*"[1] Later, also from *Katz*: "**[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected**". Additionally on *Katz*: "**GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.**". Lastly, Justice Sotomayor cites *United States v. Cuevas-Perez (2011, 7th Circuit Court)*: "**[T]he Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse**."

See also: *Carpenter v. United States (2018, SCOTUS)* – wherein Cell Site Location Information used to triangulate the location of phones may not be accessed without a search warrant as said search violates the Fourth Amendment.

While not in this jurisdiction, the Massachusetts Supreme Court stated in *Commonwealth v. McCarthy (2020)* that "**With enough cameras in enough locations, the historic location data from an ALPR system in Massachusetts would invade a reasonable expectation of privacy and would constitute a search for constitutional purposes.**"[2]. Thankfully, statute 13.824 requires the destruction of data no later than sixty days after capture (notably shorter than the one year retention period for the devices in question in the case). Later in the case, however, it is stated that "**thirty-one days of GPS monitoring was sufficient duration to conclude monitoring was search**", and "**Like both CSLI and GPS data, ALPRs circumvent traditional constraints on police surveillance power by being cheap (relative to human surveillance) and surreptitious.**"

I bring up these cases and the concurring opinion from Justice Sotomayor to dispute a common talking point from ALPR companies, who routinely say something to the affect of "people have no reasonable expectation of privacy in public spaces", which cannot be anything further from the truth. While the above cases and discussion center upon GPS trackers (or a beeper in the case of *Katz*), it is not unreasonable to draw the conclusion that a dense enough network of ALPRs that can track the every movement of a person in their vehicle. For a personal example, an ALPR operated by the Dakota County Sheriff's Office on the intersection of Ravenna Trail and 200th Street East in Ravenna Township points directly at the driveway to the house where my now deceased grandmother lived. I fully expect that the travels to and from my grandmother's house in her final days to be considered private information – the same for if I were to have driven her to her place of worship or to medical treatment centers.

1: https://www.law.cornell.edu/supct/pdf/10-1259.pdf
2: https://supreme.justia.com/cases/federal/us/565/10-1259/case.pdf

ALPRs make stalking and harassment easier; police misuses of ALPR data

In November 2025, Skagit County Superior Court in Washington State rejected the motion to keep ALPR data secret, and that ALPR data is thus marked as public data and able to be accessed through the Washington Public Records Act.[1] In response, multiple law enforcement agencies paused or stopped use of their ALPR systems.[2] I bring this up as **Minnesota has its own history of (A)LPR public data controversy**. In 2012, the City of Minneapolis released a database of over 2 million license plate scans[3] which, at the time, were considered public data. Swiftly, (then) Minneapolis Mayor R.T. Rybak worked to block the release and temporarily classify the data as non-public until after legislature could debate the issue. On September 24th, 2012, the Star Tribune posted the article "Aug. 17, 2012: City cameras track anyone, even Minneapolis Mayor Rybak"[4] where strib **reporters combed through the database and created a list of locations where Mayor Rybak had been spotted visiting – this list, unlike the original article in non-archived form, is still available to this day**[5].

If the above doesn't persuade you into believing that this treasure trove of data is ripe for abuse, the following are real cases of stalking, harassment, and abuse perpetrated by police officers with their ease of access into mass surveillance data like ALPR data.
1. 2012: Former Twin Cities police officer received one million dollar settlement after "**officers looked up her private driver's license data hundreds of times**"[6] (driver's license data).
2. 2013: Lakeville private eye latest to sue over misuse of DVS records[7] (driver's license data).
3. 2025: **Georgia police chief arrested for using Flock cameras for stalking and harassment**[7] (ALPRs).
4. 2023: **Sedgwick (Kansas) police chief tracked ex-girlfriend 164 times using license plate cams**[8] (ALPRs).

The latter two cases bring into question the chain of command for allowing outside access to ALPR data (statute 13.824 states authorization must come from the highest ranking member of the law enforcement agency, which in this case would have been the perpetrator).

1: https://www.eff.org/deeplinks/2025/11/washington-court-rules-data-captured-flock-safety-cameras-are-public-records
2: https://www.snoho.com/news/2025/dec/03/everett-is-keeping-its-flock-cameras-running-as-other-cities-pause-here-is-why/
3: https://www.startribune.com/rybak-asks-state-to-keep-car-license-data-private/183453451
4: https://web.archive.org/web/20221006052106/https://www.startribune.com/aug-17-2012-city-cameras-track-anyone-even-minneapolis-mayor-rybak/166494646/
5: https://maps.google.com/maps/ms?msid=200203856994297696125.0004c763c06e0f430b233&msa=0&ll=44.980585,-93.246803&spn=0.089125,0.222988
6: https://www.twincities.com/2012/12/06/former-twin-cities-police-officer-who-won-1-m-in-settlements-over-cops-peeking-at-her-license-data-appears-on-today-show-w-video/
7: https://www.startribune.com/lakeville-private-eye-latest-to-sue-over-misuse-of-dvs-records/197904781
8: https://lookout.co/georgia-police-chief-arrested-for-using-flock-cameras-for-stalking-and-harassment-searched-capitola-data-earlier-this-year/story
9: https://www.kake.com/home/sedgwick-police-chief-tracked-ex-girlfriend-164-times-using-license-plate-cams/article_21fdfdba-5dc5-11ef-95c4-8be8baa3f10c.html

ALPR false positives destroying lives of ordinary citizens

On July 24th, 2025, CBS reported multiple cases of false positive results from ALPRs leading to wrongful stops, abuse of ALPR technology, and aforementioned stalking from police officers using ALPR data[1]. These cases are:
1. 2018: Two brothers on their way to their parents for Thanksgiving are **held at gunpoint by a group of police officers after an ALPR falsely identified their vehicle as being stolen**.
2. 2024: **A twelve year old is handcuffed after an ALPR misread the last digit** of their older sister's license plate as a '7' instead of a '2' in Española, New Mexico.
3. A month later in the same jurisdiction, a seventeen year old honors student is **held at gunpoint after officers mistook their vehicle for one associated in an armed robbery**.
4. 2020: A mother and her family, including her six year old daughter, are pulled over in Aurora, Colorado and **held at gunpoint while forced to lie down on hot pavement. The culprit is an ALPR device that mistook their vehicle for a stolen motorbike registered in Montana**. This incident led to a **$1.9 million settlement** from the city four years later.

1: https://www.cbsnews.com/news/license-plate-readers-alpr-mistakes/

Recommendations for improving compliance for statute 13.824

While we are long past the time to debate its legality in the first place, I would personally recommend the Legislative Committee on Data Practices to weigh the advantages that law enforcement agencies receive from using ALPRs against the terrible cybersecurity flaws, psychological toll that false positives may inflict, and fourth amendment privacy concerns that modern ALPR devices bring with them. I would personally prefer banning ALPR devices statewide, however I am aware it is an unreasonable request. Thus, I have created a list of recommendations to help fight against the negative consequences that usage of ALPRs bring.

1. Require any ALPR hardware and software to be vetted either by MNIT or an independent cybersecurity penetration testing team to ensure proper compliance with the statute's provisions as well as general cybersecurity posture. It is unacceptable to be putting the life and liberty of Minnesotans and other citizens at risk due to a large network of incredibly insecure surveillance devices.
2. Require law enforcement agencies to conduct an audit within 90 days of the first use of their ALPR devices or software to make sure their systems are set up in a way that is compliant with Minnesota law. I am also in favor of shortening the length of time between audits to an annual basis instead of biennially.
3. Tighten the ability for law enforcement agencies to withhold the location of their ALPR devices by stating the location falls under "security information". Have the commissioner of administration have the final say on whether the agency is being over-judicious with their classification.
    1) For instance, the University of Minnesota Police Department (which is required by law to undergo the same restrictions as other agencies per statute 13.32) has the location of all of their stationary ALPR devices from the list maintained by the Bureau of Criminal Apprehension. In my opinion, this isn't a problem if, for example, they were using an ALPR device to monitor a police department parking ramp for people who accidentally drive in, but at least they should list a few of their ALPR devices that are within public view from the street, as they have the same expected level of secrecy as every other department's ALPR devices.
        1. The transparency portal for the UMPD shows (as of December 8th, 2025) that there were 224,500 license plates detected within the past 30 days[1]. They also have over twice the amount of ALPR devices than Hennepin County as a whole[2].
        2. The locations of (at least some) of these ALPR devices are so easy to find that an anonymous member of my community found some of them while driving around:
            1. Washington Ave, east of 19th Ave S
            2. 15th Ave SE at 8th St SE
            3. 15th Ave SE at Como Ave
            4. University Ave SE, west of Huron Blvd SE
            5. Huron Blvd SE at Fulton St SE (northbound)
            6. Huron Blvd SE at Fulton St SE (southbound)
4. More stringent requirements for search reasons should be required. While there are strict requirements for searches of active criminal investigations, any other searches have little to no restrictions behind them, so you tend to see a number of search reasons like "sus" or "suspect" which are incredibly opaque[3].
5. Wording on what constitutes an ALPR device that is privately owned but is applicable to 13.824 would go a long way for Minnesotans to figure out what is and what isn't restricted by the statute. I'd like to see further restrictions on private ALPRs in general as well, but I'm not sure where the fine line between consumer privacy advocacy starts and too much government overreach ends.
6. 13.824 subdivision 8 should be expanded to include the following data points:

1) Total number of stationary ALPR devices operated by the agency
2) Total number of non-stationary ALPR devices operated by the agency (in effect, attached to police vehicles)
3) MGDPA contact information for the agency
4) Prior locations of stationary ALPRs (this information is already required for biennial audits)
5) Date of first usage or erected date in addition to the date which the agency contacted the Bureau of Criminal Apprehension (to make oversight of subdivision 8 easier and more public).
6) Require live audit information (similar to what is seen on transparency.flocksafety.com, see below link for UMPD) to be made public and linked on said list.
7) Require agencies to disclose sources of funding for their ALPR devices (e.g. New Prague's grant from the Department of Homeland Services[4]).

1: https://transparency.flocksafety.com/university-of-minnesota-mn-pd-twin-cities
2: https://transparency.flocksafety.com/hennepin-county-mn-so
3: https://transparency.flocksafety.com/edina-mn-pd (including the image following the last of these sources)
4: https://github.com/SChapin97/Minnesota-ALPR-Documentation/blob/9ef0bb57d6c3e11e4b1c63169d97aad110828c92/public_letters/letters_to_congress/resources/new_prague_alpr_dhs_grant.png