Legislative Data Practices Commission Testimony 12.11.2025

Chairs Scott and Feist, House and Senate Members of the Data Practices Commission,

The ACLU of Minnesota appreciates this opportunity to provide additional information regarding Automatic License Plate Readers (ALPRs) in advance of your December 11, 2025 hearing.

In 2015, ACLU-MN supported the statewide regulation of ALPRs noting that they were a "legitimate tool when used for narrowly tailored law enforcement purposes, such as identifying vehicles that are stolen, involved in a crime, or associated with fugitives"; however, ALPRs were then "being used to collect and store information not just on people suspected of crimes, but on every single motorist" and that the cameras were "increasingly becoming a tool for mass routine location tracking and surveillance."

The Problem:

- Growing usage of ALPR facilitated by private companies
    - Centralized data by third parties, easily accessible
- Flock Safety – the largest company in the ALPR space. **Data collected by Flock and stored on Flock servers used to be limited to local use. Now, however, it is frequently, by default, shared with law enforcement and other Flock customers nationwide** (who, in turn, may share access to it with non-Flock customers by running searches on their behalf).
- This is a massive amount of data with broad, open-ended access to Minnesotans' data that is prohibited by the MNGDPA.
- Early **data requests reviewed by the ACLU-MN show** that in a 30-day period one Minnesota police department, with only 10 cameras, received over 11,300 searches from police departments around the nation. This is not the level of privacy protection contemplated in the ALPR statute, Minn.Stat. 13.824.

Contracts reviewed by the ACLU-MN between Flock and Minnesota law enforcement provide that:

- Flock Services, as defined, includes the sharing of still images, video, audio, and other data (Footage) captured by Flock cameras.

- Flock may use this Footage to train its algorithms and other private business purposes.
- Flock, at its discretion, may disclose Footage to other entities "if Flock has a good faith belief that such access, use, preservation or disclosure is reasonably necessary to comply with a legal process, enforce this Agreement, or detect, prevent or otherwise address security, privacy, fraud or technical issues, or emergency situations."

The drafters of Minnesota's ALPR statute clearly contemplated the risks of a vast centralized database – Minn.Stat. 13.824 subd.2(c) expressly prohibits the creation of a central state repository of ALPR data. **Instead, and circumventing the intent of that provision, law enforcement agencies are utilizing a private, third-party central repository of all ALPR data accessible by any Flock end-user.**

The ACLU of Minnesota is concerned about the growing reliance and use of Flock cameras. Minnesota Data Practices' Law requires that access to ALPR data (1) be authorized in writing; (2) for a "legitimate, specified, and documented law enforcement purpose"; and (3) "include a record of the factual basis for the access and any associated case number, complaint, or incident..." (Minn.Stat. 12.824 subd.7(b)). By searching the central Flock repository, using a pre-designed menu of drop-down choices, law enforcement agencies around the country are able to review the data with Flock – not local law enforcement – serving as the decider of what constitutes a "legitimate" law enforcement purpose not to mention there are often no case, complaint, or incident numbers submitted with theses searches.

Numerous abuses have been documented, including:

- Dallas police searched 6,674 different individual Flock camera networks composed of 77,771 total devices for ICE and Enforcement and Removal Operations (ERO)
- A California police department searched AI-enabled, ALPR cameras in relation to an "immigration protest".
- Customs and Border Protection (CBP) regularly searched more than 80,000 Flock ALPR cameras, according to data released by three police departments. One of the police departments said it did not know or understand that it was sharing data with CBP.
- Johnson County Sheriff's Office in Texas searched a nationwide network of Flock cameras to look for a woman who self-administered an abortion.
- A Sedgwick, Kansas, police chief used Flock Safety license plate readers to track his ex-girlfriend's and her new boyfriend's vehicles 228 times over four-plus

months and used his police vehicle to follow them out of town. Similar incidents occurred in another Kansas town and in Florida.

Additionally, Flock data collects additional data exceeds the limits of Minnesota statute. Bumper stickers and other vehicle details are collected and may be searchable contravening the limits of Minn.Stat. 13.824 subd.2(a). Industry research group IPVM found that Flock cameras misidentify the state of the license plate nearly 10% of the time.

Policy Recommendations:

- Shorten 60 day retention period for holding data
- Require Law enforcement agencies to store data locally
    - On agency controlled servers that are not accessible nationwide
- Require queries of LE to go through local agencies not third party
- Require strict adherence to the MN Data Practices Act

We hope that the Legislature will take these concerns about Minnesotans' data seriously. The drafters of our ALP statute did not intend for a centralized database of Minnesotans driving records, nor did they envision outsourcing compliance with our data Practices Act to a third-party private-equity-backed surveillance firm.

Thank you.

John Boehler

Policy Counsel, ACLU-MN