

United States Senate

WASHINGTON, DC 20510

September 21, 2026

The Honorable Todd Blanche
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, D.C. 20530

Dear Attorney General Blanche,

We write with great concern over widespread reports regarding the misuse of automatic license plate reader (ALPR) systems, which may be purchased with federal funding. Specifically, reporting indicates that in dozens of cases across the country, police officers have improperly and, in some cases, illegally used ALPR technology to stalk and harass their current, former, or prospective romantic partners.¹ While law enforcement agencies around the country appropriately use ALPR for legitimate public safety purposes including the investigation of violent crime and the location and recovery of missing and abducted persons, misuse of these systems undermines the public's confidence in the technology. We, therefore, write to request information about the Department of Justice's (DOJ) funding and oversight of such systems to prevent such misuse and ensure compliance with applicable federal statutes and regulations.

State and local law enforcement agencies have widely adopted ALPR systems in recent years to conduct traffic enforcement and support criminal investigations.² Flock's ALPR network, the largest in the country, currently contains more than 120,000 cameras across 49 states, with 140,000 monthly active users.³ ALPRs perform billions of scans of vehicles in the U.S. per month, converting those scans into searchable data on the vehicle's features, its location, and the time.⁴ This data is then uploaded into databases and retained for a certain period depending on state laws and regulations, sometimes as long as several years.⁵ In some cases, the agency can also choose to share its local data with other law enforcement agencies across the country.⁶

¹ Drew Harwell, Douglas MacMillan & Aaron Schaffer, *How Rogue Officers Turned a Nationwide Camera Network Into a Tool For Stalking*, The Washington Post (Aug. 2, 2026), <https://www.washingtonpost.com/technology/2026/08/02/how-police-officers-used-vast-network-cameras-spy-their-exes>.

² See *Automated License Plate Readers: Market Survey Report*, U.S. Dep't of Homeland Security, Science and Technology (Jun. 2025), https://www.dhs.gov/sites/default/files/2025-06/25_0606_st_lprmsr.pdf.

³ *The Price of "Free" LPR*, Flock (Jun. 25, 2026), <https://www.flocksafety.com/blog/the-price-of-free-lpr>; *What Happens if a Law Enforcement Officer Misuses the Flock System?*, Flock (May 19, 2026), <https://www.flocksafety.com/blog/what-happens-if-law-enforcement-misuses-the-flock-system>.

⁴ *Id.*

⁵ *What Are Automatic License Plate Reader Cameras?*, The Plate Privacy Project (2026), <https://plateprivacy.com>; *Automatic License Plate Recognition Systems: Summary of State Laws*, Legislative Analysis and Public Policy Association (Sep. 2025), <https://legislativeanalysis.org/wp-content/uploads/2025/09/Automatic-License-Plate-Recognition-Systems-Summary-of-State-Laws.pdf>.

⁶ See, e.g. Kristin Finklea & Dave S. Sidhu, *Automated License Plate Readers: Background and Legal Issues*, Congressional Research Service (Jul. 21, 2025), <https://www.congress.gov/crs-product/IF13068>.

ALPR systems thus enable law enforcement officials to identify vehicles associated with criminal activity and comprehensively track them across jurisdictional boundaries for investigative purposes.⁷

However, law enforcement officers have also faced numerous allegations of misusing ALPR systems. In Georgia, at least 20 law enforcement officers have been arrested after abusing their access to ALPR systems.⁸ Law enforcement officers in 11 other states have resigned, lost their jobs, or faced investigations after abusing ALPR systems.⁹ In total, at least 50 law enforcement officers to date have been charged with, or accused of, using ALPR systems for unauthorized purposes.¹⁰

At least 30 of these cases involve law enforcement officers stalking their current, former, or prospective romantic partners.¹¹ In one case, a police chief used an ALPR system to stalk a former partner by searching the vehicle tags for her and her daughter around 600 times over the course of thirteen months. These cases demonstrate the importance of strong guardrails and safeguards – such as appropriate access controls, auditing, supervisory review, and meaningful consequences of intentional misuse – to ensure that ALPRs’ tracking capabilities cannot be utilized by rogue bad actors to threaten, manipulate, and inflict harm on unsuspecting victims. Individuals who abuse their law enforcement access to ALPR systems to harass or otherwise harm another person should be held accountable, including through termination and criminal prosecution where warranted. They shouldn’t be permitted to undermine the legitimate use of ALPR technology to protect the public. Furthermore, the misuse of ALPR systems may violate requirements for the implementation of federal funding. This includes a requirement that federal funds and associated programs be “implemented in full accordance with the U.S. Constitution, applicable Federal statutes and regulations,” including provisions protecting public welfare.¹²

We are deeply concerned about the misuse of ALPR systems and believe that appropriate safeguards are necessary to protect against unauthorized access and abuse, including by individuals who might misuse the technology to stalk and harass their victims. We also want to ensure that funding of these technologies is paired with appropriate oversight to ensure that the funding is not used to facilitate such abuse.

⁷ *Id.*

⁸ Autumn Billings, *Georgia Has Arrested At Least 20 Officials for Misusing the Flock Surveillance Database*, Reason (Jul. 31, 2026), <https://reason.com/2026/07/31/georgia-has-arrested-at-least-20-officials-for-misusing-the-flock-surveillance-database>. See Zachary Bynum, *Another Georgia Officer Arrested Over Alleged Flock Camera Misuse as Internal Audits Continue Uncovering Cases*, CBS News (Jul. 19, 2026), <https://www.cbsnews.com/atlanta/news/another-georgia-officer-arrested-over-alleged-flock-camera-misuse-as-internal-audits-continue-uncovering-cases/>.

⁹ Alice Gibbs, *Police Accused of Misusing Flock Cameras Across 12 States*, Newsweek (Jul. 31, 2026), <https://www.newsweek.com/flock-camera-police-arrests-12263782>.

¹⁰ Harwell et al., *supra* note 1.

¹¹ *Id.*

¹² Statutory and National Policy Requirements, 2 C.F.R. § 200.300(a) (2026).

We urge the DOJ to provide guidance to state and local law enforcement agencies on how they can best prevent the misuse of ALPR technology. We also request responses to the following questions by no later than October 21, 2026.

1. How much DOJ funding has supported the purchase of ALPR systems?
2. What grant oversight and accountability mechanisms does DOJ have in place to address potential misuse and unauthorized access involving federally funded ALPR systems?
3. What, if any, DOJ training is provided to grant recipients on best practices for retaining and accessing data collected by ALPR systems to prevent misuse or unauthorized data access? Does such training address appropriate auditing, supervisory review, and consequences for intentional misuse?
4. In order to mitigate misuse or unauthorized data access, does DOJ have policies in place regarding the collection, use, storage, disposal, and access to data collected from ALPR systems operated by federal agencies?
5. Is DOJ aware of whether any state or local law enforcement officers have been accused of misconduct or illegal activity related to the use of federally-funded ALPR systems?
 - a. If DOJ becomes aware of such misconduct, what steps does DOJ take to ensure compliance with all applicable laws and regulations? Do these steps ever include financial penalties or requirements that agencies take corrective, disciplinary, or other remedial action against individuals responsible for intentional misuse?
 - b. Does DOJ require applicants for federal funding, for ALPR systems or otherwise, to disclose misuse or abuse of ALPR data? Does DOJ distinguish between misconduct by an individual user and systemic failures by a recipient agency when determining an appropriate response?
6. Has DOJ audited the use of ALPR systems within federal law enforcement agencies for non-law enforcement purposes, including stalking? What controls are in place to identify unauthorized queries and hold federal personnel accountable for misuse?

Sincerely,



Reverend Raphael Warnock
United States Senator



Katie Boyd Britt
United States Senator