Utah Privacy Commission

AUTOMATIC LICENSE PLATE READER PRIVACY CONCERNS

EXECUTIVE SUMMARY & STATUTORY AUTHORITY

Pursuant to a formal request submitted by Representative Kristen Chevrier on May 19, 2026, the Utah Privacy Commission (Commission) convened the ALPR Task Force to review operational and privacy considerations regarding Automatic License Plate Reader (ALPR) systems. This report evaluates proposed policy and statutory improvements in connection with 1st Substitute H.B. 327 License Plate Reader Amendments (2026 General Session) and current ALPR governing statute Utah Code § 41-6A-2001 et seq., Automatic License Plate Reader System Act (Act).

The Commission exercises statutory advisory authority to *"review the privacy implications and civil liberties concerns of government privacy practices"* and to *"develop guiding standards and best practices with respect to government privacy practices"* (Utah Code § 63A-19-204(1)(b) and (d)). While formal statutory language is drafted by the Office of Legislative Research and General Counsel (OLRGC) at the direction of sponsoring legislators, the Commission provides this advisory to evaluate fundamental civil liberties risks and recommend necessary privacy guardrails to inform legislative consideration; this is not legal advice. As a threshold matter, the legislature will need to determine to what extent governmental ALPR deployment and use may constitute unreasonable searches, including both those that violate the Fourth Amendment of the United States Constitution and Article I, Section 14 of the Utah Constitution and those that may be constitutionally permissible but which violate notions of good public policy. To the extent that the Legislature believes the deployment and use of ALPR technology is constitutional and good public policy, it should still enact a comprehensive statutory guardrails governing all operational aspects of the technology.

The Commission acknowledges that there are benefits that can come from ALPRs, including to public safety and criminal investigations. In particular, such technologies can assist in the hot pursuit of suspects in cases of serious crimes, and can even help locate suspects a reasonable time after a crime occurs. In some instances, historic ALPR data may produce relevant evidence. However, whether and to what extent those benefits justify certain uses of the ALPRs, and in particular lengthy data retention periods, is an important question that has not been adequately studied. Any such benefits must be carefully balanced against the privacy implications and civil liberties concerns that are analyzed and addressed in this report. Since ALPRs can provide the technical feasibility to facilitate automated mass surveillance, capable of aggregating comprehensive, time-stamped records of all Utahns' daily movements – as opposed to a specific individual who may be the target of a criminal investigation for example – they pose profound risks to privacy, associational freedoms, and due process. Protection of individual constitutional rights and reasonable expectations of privacy must be the state's default posture.

AUTOMATIC LICENSE PLATE READER PRIVACY CONCERNS

These guiding standards cannot be confined solely to standalone law-enforcement traffic cameras; they must strictly govern the expanding convergence of ALPR with multi-sensor surveillance integrations, emerging technologies, such as AI profiling capabilities, advanced analytical platforms, and any public-private networks deployed by governmental or commercial entities to monitor public spaces.

In direct response to the five inquiries submitted by Representative Chevrier, the Commission submits factual determinations and recommendations on:

1) Accuracy Standards for License Plate Reader Systems.
2) Logging, Auditing, Reporting, and Accountability Mechanisms.
3) Hotlist Accuracy and Reliability Standards.
4) Government Access to Private Surveillance Networks and Third-Party Data.
5) Ownership, Control, and Governance of Governmental LPR Data.

STAKEHOLDER CONSULTATION & REVIEW PROCESS

The review process incorporated comprehensive input from privacy groups, ALPR vendors, state and local law enforcement entities, including the Utah Department of Public Safety (DPS), the Utah Chiefs of Police Association, the Utah Sheriffs' Association, and Commissioners Chad Jensen (Cache County Sheriff) and Ryan Arbon (Weber County Sheriff). Specifically, each member of the task force contributed content to this report from their notes from discussions with stakeholders and from their independent research. Task force members then discussed multiple proposals and edits with the chair of the task force reviewing all suggested changes. With four of the five task force seats filled during the review period, suggestions were accepted if at least two members supported the change. The draft report was then reviewed on September 30th by the full Utah Privacy Commission and changers were made subsequently in response to that review before the final document was approved by the UPC on October 14th.

BRIEF INTRODUCTION TO ALPRs

The subject matter of this report is focused on "ALPRs," and associated aspects, e.g., technologies, systems, and data.

AUTOMATIC LICENSE PLATE READER PRIVACY CONCERNS

SUBSTANTIVE POLICY RECOMMENDATIONS

1) Accuracy Standards for License Plate Reader Systems

Policy Recommendations:

- Establish baseline testing procedures and accuracy rates for ALPR systems to ensure reliable performance prior to further deployment or continued operation of existing ALPR systems beyond a reasonable evaluation period.
- Require mandatory human-in-the-loop verification of all ALPR alerts before any law enforcement action is taken based upon an alert, such as a "hot list stolen vehicle alert."
- Ban or severely restrict the use of technology that excludes ALPR tracking for specifically identified vehicles.
- Mandate technological safeguards, such as end-to-end encryption between the ALPR collection devices and appropriately authorized State of Utah personnel to protect ALPR data from unauthorized access.
- Evaluate consistent statewide privacy and cybersecurity requirements through the state's cooperative contracting process, or the use of mandatory standardized provisions approved by the appropriate Utah governmental entities – including the Utah Division of Technology Services and the Utah Division of Purchasing – that accounts for the same privacy and cybersecurity requirements, for ALPR systems procured or contracted for by governmental entities, ensuring alignment with the NIST Privacy Framework and Criminal Justice Information System (CJIS) standards. Explicitly state that any contract terms that do not comply with the standardized Utah provisions or any Utah data privacy laws are void and unenforceable.

Practical Rationale:

- Formal baseline testing methods, accuracy benchmarks, and human-in-the-loop verification ensure system reliability and minimize misidentification before law enforcement intervention.
- Statewide contracting requirements establish baseline standards for data security, access control, encryption, retention, deletion, auditability, incident reporting, data ownership, data sharing, and vendor accountability.

2) Logging, Auditing, Reporting, and Accountability Mechanisms

Policy Recommendations:

- Require that all configuration changes, settings changes, searches, requests, and approvals be recorded in an immutable audit history that cannot be altered or deleted prior to legal retention schedules.
- Require ALPR systems to maintain these immutable records subject to agency oversight and independent state auditing.
- Define an appropriate level of public transparency, maintaining log retention periods and access rules consistent with the Utah Government Records Access and Management Act (GRAMA).
- Maintain meaningful accountability for intentional misuse under Utah law, ensuring peace officers who knowingly misuse ALPR systems remain subject to professional consequences, including potential POST decertification and criminal penalties, while commercial providers failing to comply face financial penalties and contractual remedies.
- Require annual independent security and privacy reviews of ALPR systems that are reported to the Legislature and the Utah Privacy Commission to keep them informed so that pertinent recommendations may be raised and appropriately addressed.

Practical Rationale:

- Independent auditing and statutory accountability mechanisms ensure compliance across both government entities and private software vendors.
- Public transparency promotes community trust and aligns directly with NIST SP 800-53 Control AU-9 and CJIS Security Policy § 5.4.5.

3) Hotlist Accuracy and Reliability Standards

Policy Recommendations:

- Mandate human verification (human-in-the-loop) of ALPR alerts before enforcement action is taken based upon a hotlist alert.
- Establish a privileged-access model for historical ALPR data requiring secondary approval when a search is conducted. Under this model, an authorized user requesting a search must document the purpose of the search and receive approval from a separate authorized supervisory or privileged user across all historical searches.

Practical Rationale:

- Historical searches present elevated privacy risks regarding longitudinal tracking of individuals' daily movements. Requiring documented justification and independent supervisory authorization prevents arbitrary querying and establishes internal agency oversight.

4) Government Access to Private Surveillance Networks and Third-Party Data

Policy Recommendations:

- Restrict commercial vendors from using or accessing Utah ALPR data for AI training, model development, or machine learning purposes.
- Support existing prohibitions on commercial sharing of government ALPR data, except pursuant to a warrant or court order based on specific and articulable facts.
- Direct the State of Utah to terminate existing contracts, and preclude future contracts, with vendors who craft Terms of Service provisions that attempt to circumvent Utah's ownership, access, and retention requirements.
- Prohibit ALPR data collected by or on behalf of a Utah governmental entity from being contributed to national or international data aggregation, storage, or analysis service that co-mingles Utah data with other non-Utah jurisdictions.

Practical Rationale:

- Historical reviews identified instances where governmental entities considered or implemented data sharing arrangements involving third-party analytical platforms, highlighting the need for clear statewide ownership rules.
- Commercial vendor platforms must not monetize or repurpose taxpayer-funded public safety data for their own benefit and purposes.
- Co-mingling Utah data in national or international services creates an inherent inability to control access to, distribution of, and mandatory deletion under Utah data retention laws.
- Access to potentially exculpatory ALPR information must be preserved for criminal defendants through appropriate legal processes.

5) Ownership, Control, and Governance of Governmental LPR Data

Policy Recommendations:

- Establish baseline ALPR maximum data retention at 21 days statewide. Longer retention of individual records outside of the general ALPR databases would be permitted as needed

under other appropriate retention schedules, for example for case-specific enforcement and litigation purposes.

- Direct appropriate government entities, such as the Department of Criminal Justice and the Department of Public Safety, to coordinate a pilot study to evaluate whether empirical data can establish a clear justification of the utility of access to ALPR data for a particular retention period. The study should allow participation by law enforcement agencies and other government entities who use ALPR systems. The study should permit participants to use an extended 9-month maximum retention period, with a sunset date of June, 2028, after which time (in the absence of further legislation) the retention period for all governmental entities would be a maximum of 21 days. Study participants would be required to evaluate the average usage/access timelines for ALPR data across crime categories, accommodating varying investigative needs, to show the specific contribution of ALPR data to a successful investigation or case resolution. Special attention should be given to analyzing the role that ALPR data played in an investigation. In particular, data should be developed to show the extent to which serious crimes would not have been solved "but for" the use of historic ALPR records. The study should also clearly delineate uses of ALPR data for serious crimes. The findings of the participants should quantitatively demonstrate evidence for a recommended retention period.
- Enact standards that ensure ALPR data collected by or on behalf of a Utah governmental entity remains under the exclusive ownership and control of the State of Utah, including raw camera data, captured plate information, associated metadata, and derived information.
- Explicitly define *commercial vendors* strictly as custodians or processors who do not acquire independent rights to use, sell, disclose, or repurpose data.

Practical Rationale:

- Retention periods across U.S. states vary widely (3 minutes to 3+ years) and fluctuate over time; empirical data regarding actual investigative utility in Utah is necessary before permanently altering statutory timeframes.
- During its review, the ALPR Task Force examined historical data sharing practices that emphasize why strict statewide ownership and non-comingling rules are essential. As a concrete example: the State of Utah previously purchased services (e.g., Palantir Gotham) from Palantir USG, Inc. pursuant to Contract No. PD2113 effective September 1, 2010. The ALPR Task Force also learned that one or more of Utah's counties, including Salt Lake County (as per Salt Lake County Criminal Justice Executive Board Meeting Minutes dated February 12, 2014), prepared Memoranda of Understanding to authorize the sharing of data (including ALPR data) with the Palantir systems. It is not currently known to what

extent any data (including ALPR data) was provided to the Palantir systems. It is currently understood (but not independently verified) that Utah's relationship with Palantir terminated in or about 2021. This potential data sharing is notable, since Palantir systems aggregate data from numerous international sources, process the data, and then resell access to the data to their international customers. It is noted that data provided to such an international data processor and reseller precludes the data remaining under the control of the State of Utah, and thereby subject to Utah law.

SUPPLEMENTARY FINDINGS & CIVIL LIBERTIES SAFEGUARDS

First Amendment Protections:

- Prohibit the use of ALPR systems for the purpose of identifying individuals or vehicles participating in First Amendment-protected activities. Prohibited activity categories include religious services or gatherings; political meetings or events; protests, demonstrations, or lawful assemblies; press or journalistic activities; petitioning government; and lawful advocacy or association.

Out-of-State Data Controls:

- Establish and enforce strict data-sovereignty protections for Utah ALPR information to ensure governmental entities outside Utah are not granted direct, bulk, or unrestricted access to Utah ALPR databases.
- Require out-of-state search requests to be evaluated through technical and administrative protocols, e.g., written agreements, prior to execution of a search, to ensure all queries comply with Utah statutory standards, including: permitted uses, secondary approval requirements, auditing controls, and a warrant accepted under Utah law.
- Limit out-of-state law enforcement queries of Utah ALPR data to investigations or prosecutions of crimes that would be felonies under Utah law, and require the requesting agency to certify the same.
- Utah government entities shall not share the ALPR data with out-of-state government entities unless ALPR data can be mutually shared pursuant to a reciprocal agreement.
- Out-of-state government entities who desire a search of ALPR data from a Utah government entity should submit such requests directly to that government entity or to Utah's Statewide Information and Analysis Center (SIAC).

AUTOMATIC LICENSE PLATE READER PRIVACY CONCERNS

Camera Placement Limitations:

- Require government-operated ALPR cameras, and those operated on behalf of government, be positioned to observe public roads, public property, and publicly observable throughways.
- Prohibit positioning ALPR cameras intentionally to monitor activity occurring on private property.
- Prohibit the placement of non-government-operated cameras on government property.