

EXECUTIVE SUMMARY & STATUTORY AUTHORITY

Pursuant to a formal request letter submitted by Representative Kristen Chevrier on May 19, 2026, the Utah Privacy Commission convened the ALPR Task Force to review operational and privacy considerations regarding Automatic License Plate Reader (ALPR) systems, specifically evaluating proposed policy and statutory improvements in connection with 1st Substitute H.B. 327 (2026 General Session).

The Commission exercises statutory advisory authority pursuant to Utah Code Ann. § 63A-19-204, which directs the Commission to “*review the privacy implications and civil liberties concerns of government privacy practices*” (§ 63A-19-204(1)(d)) and to “*develop guiding standards and best practices with respect to government privacy practices*” (§ 63A-19-204(1)(b)). 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. As a threshold matter, this advisory proceeds under the premise that if the Utah Legislature determines that governmental ALPR deployment and its operational use cases do not violate the Fourth Amendment of the U.S. Constitution or Article I, Section 14 of the Utah Constitution, comprehensive statutory guardrails should be enacted by the Legislature to govern every aspect of the technology.

While governmental entities deploy ALPR technology under the stated objective of public safety and criminal investigation, the Task Force emphasizes that operational utility cannot subordinate individual constitutional liberties. Automated mass surveillance, capable of aggregating comprehensive, time-stamped records of innocent Utahns' daily movements, poses profound risks to privacy, associational freedoms, and due process. Because individual rights must not be compromised for administrative convenience, the state's default posture should be to enforce the most restrictive statutory, retention, and technical guardrails until empirical data demonstrates that specific parameters can be adjusted without eroding individual privacy.

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, 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 Task Force 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 Jensen and Arbon.

SUBSTANTIVE POLICY RECOMMENDATIONS

Recommendation 1: Accuracy Standards for License Plate Reader Systems

- **(a) Policy Recommendation:** The Task Force recommends that policymakers evaluate and study baseline testing procedures and accuracy rates for ALPR systems to ensure reliable performance prior to any further deployment or continued operation of existing ALPR systems beyond a reasonable evaluation period. Additionally, to mitigate potential system error rates and ensure ALPR misidentifications are caught early, the Task Force recommends mandatory human-in-the-loop verification of all ALPR alerts before any law enforcement action is taken based upon an alert. Also, the Task Force recommends policymakers require technological safeguards to protect ALPR data from unauthorized access, such as end-to-end encryption between the ALPR collection devices and appropriately authorized State of Utah personnel. The Task Force further recommends evaluation of consistent statewide privacy and cybersecurity requirements through the state's cooperative contracting process for ALPR systems procured or contracted for by governmental entities and recommends they align with NIST Privacy Framework and CJIS
- **(b) Practical/Legal Rationale:** Establishing formal baseline testing methods, accuracy performance benchmarks, and human-in-the-loop verification ensures system reliability and minimizes misidentification before law enforcement intervention. Statewide contracting requirements establish minimum baseline standards for data security, access control, encryption, retention and deletion, auditability, incident reporting, data ownership, data sharing, and vendor accountability, ensuring system reliability before law enforcement intervention.

Recommendation 2: Logging, Auditing, Reporting, and Accountability Mechanisms

- **(a) Policy Recommendation:** The Task Force recommends that policymakers consider requiring that all searches, requests, and approvals be recorded in an immutable audit history that cannot be altered or deleted prior to legal retention schedules. The Task Force recommends evaluation of requirements for ALPR systems to maintain these immutable records subject to agency oversight and independent state auditing. The Task Force recommends that policymakers define an appropriate level of public transparency. The task force recommends these logs maintain retention periods and access consistent with the Utah Government Records Access and Management Act. The Task Force also recommends maintaining meaningful accountability for intentional misuse under current 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.
- **(b) Practical/Legal Rationale:** Independent auditing and statutory accountability mechanisms ensure compliance across both law enforcement personnel and private software vendors. Public transparency promotes community trust. This aligns with NIST SP 800-53 Control AU-9 and CJIS Security Policy §5.4.5.

Recommendation 3: Hotlist Accuracy and Reliability Standards

- **(a) Policy Recommendation:** The Task Force recommends evaluation of mandatory human verification (human-in-the-loop) of ALPR alerts before enforcement action is taken based upon a hotlist alert. The ALPR Task Force also recommends policymakers consider whether access to historical ALPR data should follow a privileged-access model requiring secondary approval when a search is conducted. Under this approach, an authorized user requesting a search would document the purpose of the search and receive approval from a separate authorized supervisory or privileged user when accessing historical ALPR information across all historical searches.
- **(b) Practical/Legal Rationale:** Historical searches present elevated privacy risks regarding longitudinal tracking. Requiring documented justification and independent supervisory authorization prevents arbitrary querying and establishes internal agency oversight.

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

- **(a) Policy Recommendation 1:** The Task Force recommends policymakers should consider restricting commercial vendors from using or accessing Utah ALPR data for AI training, model development, or machine learning purposes. The Task Force supports the current prohibitions on commercial sharing of government ALPR data, except pursuant to a warrant or court order based on specific and articulable facts. The Task Force recommends that the State of Utah terminate existing contracts (and not enter into future contracts) with vendors who craft Terms of Service entries that attempt to circumvent Utah's ownership, access, and retention requirements.
- **(b) Policy Recommendation 2:** The Task Force recommends that ALPR data collected by or on behalf of a Utah governmental entity be prohibited from being contributed to national or international data aggregation, storage, or analysis service that co-mingles Utah data with other non-Utah jurisdictions due to the inherent inability to control access to, distribution of, and perform the required deletion under Utah data retention requirements.
- **(c) Practical/Legal Rationale:** Historical review identified instances where entities considered or implemented 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. Access to potentially exculpatory ALPR information must also be preserved for criminal defendants through appropriate legal processes.

Recommendation 5: Ownership, Control, and Governance of Governmental LPR Data

- **(a) Policy Recommendation 1:** Rather than immediately reducing Utah's current 9-month retention period, the Task Force recommends establishing baseline ALPR data retention at 21 days, with an allowance of up to 9-months retention period for agencies willing to participate in a state study coordinated through the Department of Criminal Justice. This study will evaluate average usage timelines across Utah law enforcement agencies, accounting for specific crime categories to accommodate varying investigative needs. To ensure this expanded retention window remains strictly temporary, policymakers should establish a defined sunset date for the study period. Data gathered during this window will guide the Legislature in enacting a permanent, evidence-based retention framework.
- **(b) Policy Recommendation 2:** The Task Force recommends evaluation of standards ensuring that ALPR data collected by or on behalf of a Utah governmental entity remains under the ownership and control of that governmental entity, including raw camera data,

captured plate information, associated metadata, and derived information. The Task Force recommends that policymakers consider defining commercial vendors strictly as custodians or processors who do not acquire independent rights to use, sell, disclose, or repurpose data.

- **(c) Practical/Legal Rationale:** While 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 altering statutory timeframes. During this initial review period, the ALPR Task Force learned that 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:** The Task Force recommends that policymakers consider prohibiting the use of ALPR systems for the purpose of identifying individuals or vehicles participating in First Amendment-protected activities, including 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:** The Task Force recommends evaluation of 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. The Task Force recommends policymakers consider requiring out-of-state search requests to be evaluated through technical and administrative protocols prior to execution to ensure queries comply with Utah's statutory standards (e.g., a warrant accepted under Utah law), permitted uses, secondary approval requirements, and auditing controls.

- **Camera Placement Limits:** The Task Force recommends that policymakers consider standards requiring government-operated ALPR cameras to be positioned to observe public roads, public property, and publicly observable throughways, and not intentionally positioned to monitor activity occurring on private property.