

Utah House of Representatives

Rep. Kristen Chevrier | House District 54

May 19, 2026

Members of the Utah Privacy Commission,

Over the past several years, governmental entities across the country have rapidly adopted increasingly sophisticated surveillance and monitoring technologies without comprehensive governance frameworks in place to adequately manage the risks such technologies pose to individual liberty, privacy, due process, and constitutional freedoms. While these technologies may provide legitimate public safety and operational benefits, they also create novel risks that demand careful oversight, clear legal guardrails, and transparent accountability mechanisms.

As a member of the Utah Legislature, I am deeply concerned that the pace of technological deployment is outstripping the development of meaningful governance standards. Utah can lead the nation in creating balanced, rights-preserving frameworks that recognize both the legitimate use cases of technology and the constitutional liberties of the individuals whom government serves.

Accordingly, pursuant to the Utah Privacy Commission's authority to:

- review governmental entity privacy practices under Section 63A-19-204(1)(a)(i);
- develop guiding standards and best practices with respect to government privacy practices under Section 63A-19-204(1)(b); and
- review the privacy implications and civil liberties concerns of government privacy practices under Section 63A-19-204(1)(d)

I respectfully request that the Commission formally review the practices, standards, privacy implications, and civil liberties concerns associated with automatic license plate reader (LPR) technologies and recommend amendments or improvements to the most recent version of my 2026 General Session legislation, 1st Substitute H.B. 327, License Plate Reader and Data Retention Amendments.

I would greatly appreciate the Commission conducting this review and providing formal recommendations, including a vote on proposed bill language or legislative changes, on or

before September 30, 2026, so that legislation incorporating Utah Privacy Commission recommendations may be prepared for the 2027 General Session.

As part of this review, I ask the Commission to specifically consider several novel risks and policy questions for which there is currently little or no mature model legislation nationwide, and where Utah has an opportunity to establish thoughtful standards and best practices.

Accuracy Standards for License Plate Reader Systems

One of the most significant concerns surrounding LPR technology is the potential for inaccurate reads, false positives, and flawed hotlist matching to result in innocent individuals being stopped, investigated, detained, or otherwise harmed by governmental action. Errors in optical character recognition, poor image quality, adverse weather conditions, varying plate designs, and outdated or inaccurate databases can all contribute to harmful outcomes.

Recent reporting has demonstrated the real-world consequences of inaccurate LPR systems, including innocent individuals being subjected to police encounters and investigations because a license plate reader system incorrectly identified a vehicle. See, for example, the Electronic Frontier Foundation article describing the human toll of ALPR errors: [EFF Article on ALPR Errors](#)

The current legislation attempts to establish minimum statewide standards for independent third-party testing, accuracy evaluations, and minimum operational performance thresholds for governmental LPR systems. These provisions include requirements related to character-level accuracy, full-plate accuracy, false positive rates, and disaggregated error testing across differing plate types and imaging conditions.

I ask the Commission to evaluate whether these standards are sufficient, whether additional independent testing or auditing requirements are warranted, and whether Utah should establish stronger statewide baseline requirements before such systems may be deployed or expanded.

Logging, Auditing, Reporting, and Accountability Mechanisms

LPR systems create substantial risks of misuse if governmental entities lack strong logging, auditing, and oversight controls. Without detailed audit trails and reporting mechanisms, inappropriate access, stalking, personal misuse, unauthorized surveillance, or unlawful searches may go undetected.

Recent reporting has highlighted instances where law enforcement personnel allegedly used LPR systems to stalk romantic interests or otherwise misuse sensitive surveillance tools for personal purposes. See: [Institute for Justice Article on LPR Misuse](#)

The legislation attempts to address these concerns by requiring LPR systems to automatically generate detailed reports documenting searches, alerts, user identifiers, stated purposes, case numbers, camera locations, and related information.

I ask the Commission to evaluate what the minimum acceptable logging, auditing, reporting, retention, inspection, and accountability standards should be to ensure that governmental entities use these systems only within the confines of the law and that meaningful review and enforcement mechanisms exist when misuse occurs.

Hotlist Accuracy and Reliability Standards

The reliability of hotlists used in conjunction with LPR systems presents another significant civil liberties concern. Inaccurate, stale, improperly maintained, or overly broad hotlists can result in innocent individuals being stopped or investigated based on faulty information.

Recent examples have demonstrated how poor hotlist maintenance and inaccurate data can result in harmful law enforcement encounters. See: [9News Article on Flock and Hotlist Errors](#) The legislation attempts to establish minimum standards for hotlist governance, including requirements that hotlists be updated at least every 24 hours and that law enforcement agencies reasonably attempt to confirm the accuracy of a match before stopping or engaging a vehicle occupant.

I ask the Commission to evaluate whether these protections are adequate and whether additional requirements should exist regarding hotlist validation, expiration, data quality controls, auditing, or procedural safeguards before enforcement action may occur.

Government Access to Private Surveillance Networks and Third-Party Data

I am increasingly concerned about the growing aggregation and correlation of personal data by private-sector surveillance providers and data brokers, including private LPR networks.

There is a substantial policy concern that governmental entities may increasingly rely on the third-party doctrine to purchase or obtain access to sensitive surveillance data from private companies without the same constitutional safeguards that would normally apply if the government collected the information directly.

There is also concern that many individuals do not fully understand the scope of data collection, sharing, retention, and surveillance occurring through private-sector systems. As the deployment of private LPR systems expands nationwide, the risk grows that government could effectively engage in broad location tracking and surveillance through commercial intermediaries with minimal safeguards.

The legislation attempts to address this concern by establishing warrant requirements and restricting ongoing governmental access to nongovernmental LPR systems and databases.

I ask the Commission to carefully evaluate the constitutional, privacy, and civil liberties implications of governmental access to private surveillance networks and to recommend whether Utah should establish clearer statewide standards governing governmental acquisition, purchase, or access to privately collected location and surveillance data.

For additional context regarding concerns surrounding private-sector surveillance networks, please see: [Ring and Flock Partnership Article](#)

Ownership, Control, and Governance of Governmental LPR Data

Finally, I ask the Commission to examine the issue of governmental ownership and control of LPR data. Recent changes to private vendor terms and conditions have highlighted significant concerns regarding whether vendors may attempt to assert ownership interests, perpetual usage rights, or other forms of control over governmental data.

Regardless of where Utah ultimately lands on the broader policy debate surrounding LPR technologies, I firmly believe there should never be a circumstance where a private company may take ownership of governmental records, claim perpetual rights to use governmental surveillance data, or otherwise undermine Utah's sovereignty and authority over governmental records and information systems.

Many local governmental entities lack the negotiating leverage, technical expertise, or legal resources necessary to resist problematic vendor contract provisions. The State of Utah, however, has both the authority and responsibility to establish clear statewide protections to prevent such practices and preserve public trust.

The legislation attempts to address these concerns by establishing duties of loyalty and care for providers, prohibiting the sale or profit from governmental LPR data, and limiting disclosure and sharing.

For additional context regarding these concerns, please see: [ACLU Analysis of Flock Terms and Conditions](#)

I also respectfully request that the Commission proactively engage with Utah's law enforcement community throughout this review process to ensure that the Commission fully understands both the operational realities and the civil liberties implications associated with license plate reader technologies.

In particular, I ask that Commissioner Jensen and Commissioner Arbon, who serve on the Commission in roles representing the law enforcement community, assist in ensuring that

sheriffs, police chiefs, the Utah Department of Public Safety, prosecutors, and other relevant public safety stakeholders are actively engaged in these discussions and have the opportunity to provide input regarding operational needs, investigative value, implementation concerns, accountability mechanisms, and appropriate guardrails.

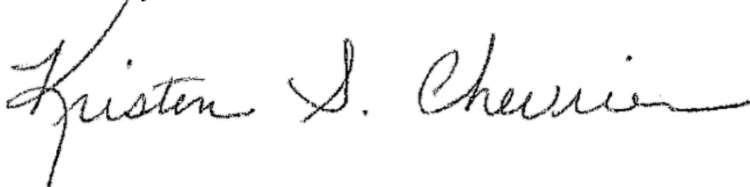
This issue is too important to approach from only a single perspective. Utah should strive to create a framework that both protects constitutional liberties and provides clear, workable standards for governmental entities and law enforcement agencies operating within the law.

I also intend to personally engage with members of the law enforcement community as part of this process and look forward to working collaboratively with all stakeholders to develop balanced, thoughtful, and durable policy solutions for Utah.

I appreciate the Utah Privacy Commission's continued work to ensure Utah remains a national leader in balancing technological innovation, public safety, governmental transparency, and constitutional liberties. I believe Utah has an opportunity to help establish a thoughtful governance model for surveillance technologies that other states may ultimately follow.

Thank you for your consideration and service.

Sincerely,

A handwritten signature in black ink that reads "Kristen S. Chevrier". The signature is written in a cursive style with a large initial 'K' and a long, sweeping underline.

Representative Kristen Chevrier
Utah House of Representatives