LITIGATION MINUTE: LICENSE TO SUE? AUTOMATED LICENSE PLATE READERS YIELD NEW PRIVACY CLAIMS

Date: 16 November 2026

US Litigation and Dispute Resolution Alert

By: Michael J. Stortz, Chief Coleman, Katy M. Ramos

Automated license plate readers (ALPRs) capture license plate information, including the plate number and the date, time, and location of the vehicle, which can create a detailed record of a vehicle's movements over time. This technology has increasingly drawn attention from the plaintiffs' class action bar, with litigation and arbitration demands driving activity in California and nationwide, with potential impacts across a range of industries. Here's what you need to know in a minute or less.

CALIFORNIA'S ALPR LAW—THE STARTING POINT

California's ALPR Privacy and Usage Act[1] (the Act) regulates entities operating ALPR systems. Among other things, an ALPR operator must maintain reasonable security safeguards, keep records of access to ALPR information, and implement and conspicuously post a usage and privacy policy addressing specified subjects, including authorized uses and users, data-sharing practices, security, accuracy, and retention.

Section 1798.90.54(a) of the Act creates a private right of action for a person "harmed" by a violation and permits recovery of actual damages or liquidated damages of US$2,500, whichever is greater, as well as punitive damages and attorneys' fees. In a putative class action challenging ALPR systems that scan thousands of vehicles, the potential aggregate exposure can quickly become significant.

BARTHOLOMEW OPENS THE DOOR

In February 2026, the first appellate decision on point, *Bartholomew v. Parking Concepts, Inc.,*[2] brought the exposure risk into focus. The plaintiff launched a putative class action, alleging that the defendant's ALPR technology collected his license plate information without adequately disclosing the required policy, in violation of the Act. The trial court dismissed the action at the pleadings stage, finding that the plaintiff failed to allege harm within the meaning of the statute.

The appellate court reversed, holding that the collection and use of license plate information without properly disclosing the usage and privacy policy can itself constitute harm, in part by infringing the plaintiff's "right to know" who collected the data at issue and how that data would be used and maintained. Under this "right to know" rationale, the plaintiff did not need to allege a data breach or improper disclosure to establish the statutory requirement of actual harm. This ruling supplies a roadmap for claims against businesses using ALPR systems, including entities that may not consider themselves operators of privacy-sensitive technology.

©2005-2026 K&L Gates LLP. All Rights Reserved.

MATA PUMPS THE BRAKES

Five months later, *Mata v. Digital Recognition Network, Inc.*[3] further defined the rule. The Mata plaintiff alleged harm based on mere collection of information in conjunction with a violation of the statute. At its core, the plaintiff's theory was that harm results from any violation of the statute. The appellate court disagreed, affirming summary judgment for the defendant.

Although the *Mata* court expressed skepticism of *Bartholomew*'s "right to know" theory, it nonetheless refrained from directly contradicting the earlier decision by delineating situations in which a usage and privacy policy exists and is simply out of compliance or is alleged to exist only to maintain the appearance of compliance.

Federal courts have since begun to adopt the approaches developed in *Bartholomew* and *Mata*.[4] As new lawsuits emerge, the caselaw will continue to shape the ALPR's "harm" requirement.

NATIONWIDE FRAMEWORKS BROADEN ALPR SCRUTINY

The Driver's Privacy Protection Act (DPPA) is the federal analogue to California's ALPR law and generally governs personal information held by state departments of motor vehicles (DMVs). The DPPA also permits individuals to pursue privacy claims against private businesses that collect, buy, sell, or use vehicle- or driver-related data.

In contrast to California, simply reading license plate numbers generally is not understood to constitute obtaining "personal information from a motor vehicle record" subject to the DPPA, but reading license plates to match ALPR data with DMV records and identify vehicle owners may trigger DPPA scrutiny. As such, any entity handling DMV-sourced data, including data obtained through intermediaries, may be exposed to significant risk.

Aside from California, eight other states have enacted legislation or executive orders that restrict, or entirely prohibit, private ALPR operations: Arkansas, Idaho, Kentucky, Maine, Missouri, New Hampshire, Oklahoma, and Rhode Island. Other states are also presently considering pending legislation on similar restrictions.

Accordingly, legal, privacy, and compliance teams should review how and why their organizations process ALPR and driver-related data and update their privacy compliance programs to reduce these risks.

TAKEAWAYS

As ALPR caselaw evolves, recent rulings offer businesses practical guidance:

1. Identify ALPR systems in use and the data they collect
2. Ensure public ALPR policies are posted, current, and reflect actual practices
3. Retain and review technology vendor agreements, including parking equipment contracts; document control over plate data collection, storage, access, retention, and sharing; and retain evidence of consumer notices

The strongest defense is a pre-litigation compliance record including clear disclosures, consistent implementation, vendor oversight, security controls, and retention limits. Our Litigation and Dispute Resolution and Data Privacy

©2005-2026 K&L Gates LLP. All Rights Reserved.

Disputes and Risk Mitigation teams can fully assess the appropriate steps to mitigate the risk of ALPR litigation in this evolving landscape.

We acknowledge the contributions to this publication from our law clerk, Grace Voissem.

FOOTNOTES

[1] Cal. Civ. Code § 1798.90.5 et seq.

[2] *Bartholomew v. Parking Concepts, Inc.*, 118 Cal. App. 5th 438 (2026).

[3] *Mata v. Digital Recognition Network, Inc.,* 121 Cal. App. 5th 1075 (2026).

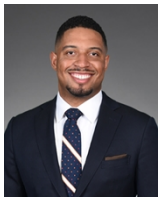
[4] *See McGinity v. Reimagined Parking LLC, d/b/a Imperial Parking*, No. 26-CV-02760-WHO, 2026 WL 2322918 (N.D. Cal. Aug. 5, 2026) (denying a motion to dismiss where plaintiff's actionable harm was based on the statutory "right to know.")

KEY CONTACTS



MICHAEL J. STORTZ
PARTNER

SAN FRANCISCO
+1.415.882.8011
MICHAEL.STORTZ@KLGATES.COM



CHIEF COLEMAN
ASSOCIATE

LOS ANGELES
+1.310.552.5051
CHIEF.COLEMAN@KLGATES.COM



KATY M. RAMOS
ASSOCIATE

LOS ANGELES
+1.310.552.5570
KATY.RAMOS@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2026 K&L Gates LLP. All Rights Reserved.