Coblentz
Patch Duffy
& Bass LLP

California Court Clarifies Standing Under the State's ALPR Law

The California Court of Appeal recently handed businesses that use automated license plate recognition (ALPR) technology an important victory, holding that a plaintiff must suffer actual harm to have standing to bring a claim under the statute. In *Mata v. Digital Recognition Network, Inc.*, 2026 WL 2085579 (Cal. Ct. App. July 20, 2026), the Court of Appeal affirmed summary judgment, holding that where a business maintains a written ALPR policy, a plaintiff must plead and prove harm distinct from the alleged statutory violation to establish liability.

Requirements of the California ALPR Statute
California law requires ALPR operators and end-users to maintain reasonable security procedures and adopt a usage and privacy policy governing the collection, use, maintenance, sharing, and dissemination of ALPR information.[1] The policy must address seven statutory specific topics, including authorized uses, access controls, employee training, security monitoring, data sharing, retention, and destruction. The statute does not otherwise restrict a private entity's collection or use of ALPR information if it maintains a compliant policy and otherwise complies with security, operational, and other statutory requirements.

The Recent *Mata* Court of Appeal Decision
Plaintiff Guillermo Mata brought a putative class action against Digital Recognition Network, Inc. (DRN), a company that provides license plate recognition services to customers and that housed more than nine billion license plate images in its ALPR system. DRN collected and maintained the images pursuant to an ALPR usage and privacy policy adopted in 2015.

Plaintiff alleged a single cause of action for violation of the ALPR statute and on behalf of a putative class composed of "[a]ll persons in the State of California whose license plate data was collected by [DRN] using an automatic plate reader." While DRN's ALPR policy included the seven items of information required by the statute, the plaintiff claimed that the purpose of the policy was to "maintain the appearance of adhering" to the ALPR statute and "to pay lip service to privacy laws without having any intention of actually complying with them."

DRN moved for summary judgment on the basis that the plaintiff suffered no actual harm. DRN conceded that it captured plaintiff's license plate data at least 15 times. Yet, DRN argued that the plaintiff had not had his identity stolen, nor had he suffered any physical injury, harm, or lost wages as a result of any conduct by DRN. Instead, he testified that the only harm he suffered was that his "privacy ha[d] been violated on multiple occasions."

The trial court held, and the Court of Appeal agreed, that actual harm was a necessary component of the statutory standing inquiry. First, under the plain language of the statute, only an individual "who has been harmed by a violation of the statute" has a private right of action to bring a lawsuit.[2] The court concluded that the required *harm* must be distinct from the statutory *violation* itself. Because the plaintiff alleged only that the violation invaded his privacy, he failed to establish the requisite harm. The legislature further provided examples of harm under the ALPR statute, including "unauthorized access or use of ALPR information or a breach of security of an ALPR system."[3] These examples require more than a mere statutory violation.

Second, the legislative history supported that interpretation. One report referred to damages in actions brought by individuals harmed by the improper use of ALPR data, while another described claims by individuals whose information was unlawfully disclosed. Both examples involved misuse or disclosure of ALPR information—not mere noncompliance with the statute.

[1] *Cal. Civ. Code § 1798.90.54*.

[2] *Cal. Civ. Code § 1798.90.54(a).*

[3] *Id.*

Mata Is In Tension With Another Recent ALPR Decision

Mata was decided shortly after *Bartholomew v. Parking Concepts, Inc.*, 118 Cal. App. 5th 438 (2026), which we previously discussed here. There, the Court of Appeal determined that the absence of an ALPR policy was a harm that could be the basis for liability under the statute. The court in *Bartholomew* concluded that collecting and maintaining ALPR information without implementing and publishing the required policy harms individuals and violates their "right to know" who is collecting their ALPR data and for what purposes they are using it.

The *Mata* court expressed its skepticism about the "right to know" harm, but distinguished *Bartholomew*'s limited holding and confined it to businesses without an ALPR policy. In other words, if a business fails to draft and display a written ALPR policy, the absence of that policy may itself satisfy the statute's harm requirement. By contrast, where a business does adopt and conspicuously post a written ALPR policy, then a plaintiff must show harm distinct from the asserted statutory violation, such as actual harm by the collection or use of the license plate data.

What Businesses Should Do Now

Together, *Mata* and *Bartholomew* provide businesses with a clearer pathway going forward. Businesses subject to the California ALPR statute applies should promptly confirm that they have an ALPR policy in place. Doing so may reduce risk of lawsuits similar to *Bartholomew* where a plaintiff can allege a bare statutory violation and will require plaintiffs to suffer actual harm to succeed.

Additionally, because these ALPR lawsuits are on the rise, businesses that fall within the law's purview should consider taking the following steps:

- Identify all locations where cameras or parking systems capture license plate information.
- Determine whether those systems create or access a searchable database of license plate information.
- Confirm whether the business is an ALPR "operator," "end-user," or both.
- Review vendor contracts to understand who collects, stores, accesses, shares, and deletes ALPR information.
- Adopt a written ALPR usage and privacy policy that includes all required statutory elements.
- Post the policy conspicuously on the business's website and make it available in writing.
- Review retention, access, audit, training, and security practices to ensure they match the posted policy.
- Periodically audit compliance, particularly when deploying new parking, security, or access-control technology.

If your company needs assistance with any privacy issues, the Coblentz Data Privacy & Cybersecurity team can help. Please reach out to Scott Hall or Phillip Wiese for further information or assistance.

Contacts

Scott Hall
Partner

415.772.5798
shall@coblentzlaw.com
www.coblentzlaw.com

Phillip Wiese
Special Counsel

415.268.0502
pwiese@coblentzlaw.com
www.coblentzlaw.com

Leeza Arbatman
Associate

415.293.6449
larbatman@coblentzlaw.com
www.coblentzlaw.com