California Court Finds Harm in Collection and Use of License Plate Information without Privacy Policy: 4 Steps Your Business Should Take

Insights
2.24.26

A California appellate court recently held that a parking garage's automated collection and use of license plate information without a publicly available privacy policy violated a state law, serving as a stark reminder for your business about the importance of maintaining and following such policies. The February 5 decision in *Bartholomew v. Parking Concepts, Inc.*, found that a plaintiff could proceed with his case brought under a California statutory scheme governing automated license plate recognition (ALPR) systems. Critically, the court found that failing to implement the public-facing privacy policy in and of itself constituted a "harm" within the meaning of the ALPR Law. For businesses with ALPR systems, here are four things to do to stay compliant and protect yourself from liability.

The Case at a Glance

Brendan Bartholomew parked his vehicle in a parking garage owned and/or operated by Parking Concepts multiple times in 2022 and 2023. When he arrived at the garage, he took a printed parking ticket that displayed his license plate number. Upon leaving, a screen on the exit kiosk displayed his license plate number and, after confirming he had paid, the barrier arm would automatically lift to allow his vehicle to exit.

Bartholomew brought a lawsuit against Parking Concepts, alleging that it automatically collected his license plate information when he parked his vehicle without having implemented or made publicly available a usage and privacy policy as required by California's ALPR Law.

Court's Decision: Lack of Policy = Harm

The court's February 5 decision allowed Bartholomew's case to proceed. The business argued that "harm" requires some type of affirmative misuse or mishandling of ALPR information, and therefore simply collecting and using the information without a requisite policy is not enough. But the court disagreed.

It held that a plaintiff need not suffer measurable monetary damages to establish harm to bring a suit under the ALPR Law. Rather, the court determined that the defendant's failure to make publicly available a usage and privacy policy constituted a "harm" within the meaning of the ALPR Law.

As the court noted: "Collecting and maintaining individuals' ALPR information without implementing and making public the statutorily required policy harms these individuals by violating this right to know."

Why This Matters For Businesses

While a plaintiff need not show monetary damages, plaintiffs suing under the ALPR Law can be entitled to liquidated damages in the amount of $2,500, punitive damages, attorneys' fees, and injunctive relief. This creates incentives for plaintiffs' counsel to bring such cases on a class action basis, even though the damages to any particular individual may be minor.

Your Next Steps

You should consider the following four steps in order to put yourself in the best possible position when it comes to ALPR claims.

1. If Your Business Has an ALPR System, Review Whether You Have a Publicly Available Usage and Privacy Policy. The court emphasized that it was the failure to have such a policy that constituted a harm. As such, the first step to mitigating risk is to ensure your business has and posts such policies publicly on your website.

2. Ensure You Comply With Your ALPR Policy. California law requires, among other things, information regarding the purposes for collecting ALPR data, security measures surrounding the ALPR system, and the length of time ALPR information will be retained. While the key issue in this case was the lack of a usage and privacy policy, it is also important to remember that an inaccurate usage and privacy policy is also a violation of the ALPR Law. Be sure your privacy policy does not overpromise and underdeliver.

3. Consider (And Reconsider) Who You Disclose ALPR Data To. While the ALPR Law does not have strict limits on the collection, use, maintenance, sharing, and dissemination of ALPR information, they should be, as the court said, "consistent with respect for individuals' privacy and civil liberties." This leeway on the usage and disclosure of ALPR data is broad, but not unlimited. Businesses should carefully consider whether the context in which they collect ALPR data or the businesses to which they disclose ALPR data could be deemed an invasion of privacy or civil liberties. This analysis will be context-specific, and the outcome may change over time in response to evolving norms.

4. Prepare For Plaintiffs to Pivot To Old Privacy Laws. The ALPR Law is yet another example of plaintiffs re-discovering older privacy laws to find a hook into your business. (The zeitgeist of this trend has been the flood of wiretapping litigation.) While the ALPR Law is one risk, make sure that your privacy compliance program is compliant on all privacy fronts. There is not a single privacy law; businesses must consider a myriad of laws with, at times, overlapping or inconsistent obligations. For California, those laws also include the California Consumer Privacy Act and the

California Invasion of Privacy Act – businesses should not and cannot assume that compliance with one law means that the business is compliant with all applicable privacy laws.

Conclusion

If you have any questions, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney on our Privacy and Cyber team. You can also visit FP's U.S. Consumer Privacy Hub for additional resources to help you navigate this area. Make sure you are subscribed to the Fisher Phillips' Insight System to receive the latest developments straight to your inbox.

Related People

Darcey M. Groden, CIPP/US
Partner
858.597.9627
Email

David Shannon, CIPP/US
Associate
615.488.7401

Email

Service Focus

Privacy and Cyber

Consumer Privacy Team

Litigation and Trials

Trending

U.S. Privacy Hub

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Silicon Valley

Woodland Hills