

YES  NO

**EXHIBITS**

CASE NO. 26 Ch 05072

DATE: 5-27-26

CASE TYPE: Class Actions

PAGE COUNT: 22

**CASE NOTE**

---

---

---

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS  
COUNTY DEPARTMENT, CHANCERY DIVISION

|  |   |                             |
|--|---|-----------------------------|
| MICHELLE ROJAS and MARISSA                 | ) |                             |
| BARRIGA, individually and on behalf of all | ) |                             |
| other persons similarly situated,          | ) |                             |
|  | ) | Case No. <u>2026CH05072</u> |
| Plaintiffs,                                | ) |                             |
|  | ) | Judge _____                 |
| v.   | ) |                             |
|  | ) |                             |
| MOTOROLA SOLUTIONS, INC.,                  | ) | <b>JURY TRIAL DEMANDED</b>  |
|  | ) |                             |
| Defendant.                                 | ) |                             |

**CLASS ACTION COMPLAINT**

Plaintiffs Michelle Rojas and Marissa Barriga (collectively, “Plaintiffs”), by and through their counsel, bring this action on behalf of themselves and all others similarly situated against Defendant Motorola Solutions, Inc. (“Defendant” or “Motorola”) based upon the factual investigation of their counsel, their personal knowledge as to facts pertaining to themselves and information and belief as to all other matters.

**NATURE OF THE CASE**

1. This is a putative class action against Defendant Motorola for violations of Plaintiffs’ and Class members’ (defined below) right to privacy, as codified under California Civil Code § 1798, *et seq.*, through the improper and unlawful operation of an automatic license plate reader (“ALPR”) system.

2. An ALPR system consists of a “searchable computerized database resulting from the operation of one or more mobile or fixed cameras combined with computer algorithms to read and convert images or registration plates and the characters they contain into computer readable data.” *See* Cal. Civ. Code § 1798.50.5(d).

FILED DATE: 5/27/2026 3:47 PM 2026CH05072

3. ALPR systems typically utilize high-speed cameras and accompanying software that record, capture, analyze and store information about vehicles' make, model, license plate numbers and GPS coordinates. Oftentimes, these cameras capture photographs of an entire vehicle, as well as the date, time and location of the vehicle, as it passes the cameras. The cameras may also capture an image of the vehicle driver and passengers and other unique characteristics of the vehicle.

4. ALPR cameras are indiscriminate. They capture images of any vehicle that passes by the ALPR cameras.

5. An ALPR system can be used to target individuals who visit sensitive locations such as immigration clinics, health centers, protests and places of worship.

6. California has determined "that the right to privacy is a personal and fundamental right protected by . . . the Constitution of California and by the United States Constitution and that all individuals have a right to privacy in information pertaining to them." Cal. Civ. Code § 1798.1. In connection therewith, California has found that: (a) "[t]he right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information . . . ."; (b) "[t]he increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information"; and (c) "[i]n order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits." *Id.*

7. Defendant is a nationwide private vendor of an ALPR system, including ALPR cameras and software that allow for the analysis of the data captured by the cameras.

8. Defendant has made, and continues to make, its ALPR system available to third parties throughout California. As a result, Defendant's ALPR cameras are installed in locations throughout California, including Merced, California (the "California ALPR Cameras").

9. The California ALPR Cameras capture license plate information of Plaintiffs and Class members each time they pass by or park near one of the cameras. Further, the California ALPR Cameras capture the GPS coordinates of Plaintiffs and Class members when the pass by or park near the cameras, as well as the date and time they pass by or park near the cameras. The captured information may be used to identify the operator or registered owner of the vehicle.

10. The California ALPR Cameras capture the information described in the preceding paragraph without notice to Plaintiffs and Class members and without their consent.

11. Defendant boasts that, based on the information captured by its ALPR cameras, users of its ALPR system can "[e]asily search for, find and review the location history of a vehicle . . . and determine where it may be located in the future."

12. Unbeknownst to Plaintiffs and Class members, Defendant's ALPR system allows for the sharing of their captured information with the federal government and state agencies outside of California, in violation of California law and Plaintiffs' and Class members' right to privacy. Among the network of entities to which Defendant allows unauthorized access of the ALPR information from the California ALPR Cameras are: (a) Customs and Border Patrol – National Targeting Center; (b) IRS Criminal Investigation; (c) United States Marshals Service; and (d) United States Secret Service.

13. Plaintiffs assert claims on behalf of themselves and all others similarly situated for Defendant's violations of Cal. Civ. Code § 1798.90.5, *et seq.*, which governs the use and operation of ALPR systems within the State of California.

## PARTIES

14. Plaintiff Michelle Rojas is a citizen of California, residing in Merced, California near the entrance to the University of California – Merced (“UC Merced”) located at Lake Road and Bellevue Road in Merced, California (the UC Merced Entrance”). At relevant times, Defendant’s California ALPR Cameras captured Plaintiff Rojas’ license plate number and geolocation data, among other personal information, when she passed by Defendant’s ALPR cameras located near the UC Merced Entrance.

15. Plaintiff Marissa Barriga is a citizen of California, residing in Merced, California. At relevant times, Defendant’s California ALPR Cameras captured Plaintiff Barriga’s license plate number and geolocation data, among other personal information, when she passed by Defendant’s ALPR cameras located near the UC Merced Entrance.

16. Defendant Motorola Solutions, Inc. is a Delaware corporation with its principal place of business located in Chicago, Illinois.

## JURISDICTION AND VENUE

17. This Court has jurisdiction pursuant to 735 ILCS 5/2-209, as Defendant is a corporation that does business within the State of Illinois.

18. Pursuant to 735 ILCS 5/2-101 and 102, venue is proper because Defendant is a resident of Cook County, Illinois.

## FACTUAL BACKGROUND

### *ALPR Systems*

19. ALPR systems consist of computer-controlled cameras, among other things, that automatically capture license plate numbers within their view, along with the location, date and time the image is captured.

20. ALPR cameras can be stationary or mobile, such as when they are affixed to a moving vehicle.

21. The information captured by ALPR cameras can include images of the vehicle to which a license plate is attached and the driver and passengers of the vehicle.

22. ALPR cameras capture information indiscriminately. ALPR system operators, like Defendant, use this information to amass profiles on the vehicles that pass by or park near their ALPR cameras to allow end-users to “search for, find and review the location history of a vehicle . . . and determine where it may be located in the future.”

23. By amassing profiles in the above-described manner, ALPR systems can be used for nefarious purposes, such as to track and locate protestors, people attending religious events or persons with a particular immigration status.

***Defendant Motorola and Its ALPR System***

24. Defendant touts itself as a “global leader in mission-critical safety and security technologies for public safety, government, including defense, and enterprise customers.” Defendant claims to “design and advance technology for more than 100,000 customers in over 100 countries . . .” Defendant claims the goal of, among other things, dismantling “silos and barriers between people and systems . . . .”

25. One of Defendant’s core business segments is video technology, which includes ALPR technology and AI-powered analytics. According to Defendant, its “video software integrates AI-powered analytics to deliver operational insights to [its] customers by bringing attention to important events within their video footage.” It is Defendant’s view that “these insights can help to proactively detect an important event in real time as well as reactively search video

content to investigate an important event that occurred in the past.” In Defendant’s words, its AI-powered analytics can use license plate recognition to “flag a vehicle of interest.”

26. Defendant claims that users of its ALPR system have access to “over 40 Billion 3rd Party Scans” and that it is the only one in the industry with a database that goes back over 17 years.

27. Defendant’s published materials regarding its ALPR system indicate that its fixed and mobile ALPR cameras can obtain vehicle data of vehicles traveling up to 150 miles per hour in the dark and can read “all plates, temporary tags, paper tags and even identify when a plate is missing.”

28. The data collected via Defendant’s ALPR system may be used to identify the driver or registered owner of the vehicle whose data is collected. Defendant’s ALPR system stores this personally identifiable information and makes it available to users of the ALPR system.

29. Defendant uses the ALPR system to collect and store ALPR data for its own commercial purposes. Defendant also makes the ALPR system available to customers, such as law enforcement agencies and commercial customers.

***Defendant’s Failures to Safeguard ALPR Information***

30. Beyond Defendant’s self-serving claims about the benefits of its ALPR system, its ALPR system has been newsworthy for its security lapses.

31. For instance, in June 2024, the Cybersecurity & Infrastructure Security Agency (“CISA”) issued an advisory regarding “Motorola Solutions Vigilant License Plate Readers,” citing vulnerabilities in Defendant’s ALPR technology that “could allow an attacker to tamper with the device, access sensitive information and credentials, or perform a replay attack.” For context, Vigilant Solutions was a provider of ALPR technology that was purchased by Defendant in 2019.

32. Further, in January 2025, an independent security researcher revealed that it was possible for people to view real-time footage and data from Defendant's ALPR cameras on the open internet without authentication. In other words, the video and data streams from the ALPR cameras could be watched without any sort of login.

33. Moreover, as alleged in more detail below, despite California law requiring ALPR operators to maintain reasonable security procedures and practices, including operational, administrative, technical and physical safeguards to protect ALPR information from unauthorized access, use, modification and disclosure, in April 2026, it was reported that the federal government and non-California agencies had access to ALPR information captured by Defendant's ALPR system despite such access and use being prohibited by California law.

#### ***California's ALPR Regulations***

34. California Civil Code § 1798.90.5, *et seq.*, regulates the operation and use of ALPR systems by ALPR operators and end-users (the "ALPR Regulations").

35. Pursuant to the ALPR Regulations, an "ALPR system" is a "searchable and computerized database resulting from the operation of one or more mobile or fixed cameras combined with computer algorithms to read and convert images or registration plates and the characters they contain into computer-readable data." Cal. Civ. Code § 1798.90.5(d).

36. Pursuant to the ALPR Regulations, a "person" is "any natural person, public agency, partnership, firm, association, corporation, limited liability company or other legal entity." Cal. Civ. Code § 1798.90.5(e).

37. Pursuant to the ALPR Regulations, an "ALPR operator" is a "person that operates an ALPR system," subject to an exception that is not applicable here. Cal. Civ. Code § 1798.90.5(c).

38. Pursuant to the ALPR Regulations, an “ALPR end-user” is a “person that accesses or uses an ALPR system,” subject to exceptions that are not applicable here. Cal. Civ. Code § 1798.90.5(a).

39. Pursuant to the ALPR Regulations, “ALPR information” is “information or data collected through the use of an ALPR system.” Cal. Civ. Code § 1798.90.5(b).

40. Pursuant to the ALPR Regulations, “public agency” means “the state, any city, county, or city and county, or any agency or political subdivision of the state or a city, county, or city and county, including but not limited to, a law enforcement agency.” Cal. Civ. Code § 1798.90.5(f).

41. According to the ALPR Regulations, an ALPR operator is required to:

- (a) Maintain reasonable security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure.
- (b)(1) Implement a usage and privacy policy in order to ensure that the collection, use, maintenance, sharing, and dissemination of ALPR information is consistent with respect for individuals’ privacy and civil liberties. The usage and privacy policy shall be available to the public in writing, and, if the ALPR operator has an Internet Web site, the usage and privacy policy shall be posted conspicuously on that Internet Web site.
- (2) The usage and privacy policy shall, at a minimum, include all of the following:
  - (A) The authorized purposes for using the ALPR system and collecting ALPR information.
  - (B) A description of the job title or other designation of the employees and independent contractors who are authorized to use or access the ALPR system or to collect ALPR information. The policy shall identify the training requirements necessary for those authorized employees and independent contractors.

- (C) A description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws.
- (D) The purposes of, process for, and restrictions on, the sale, sharing, or transfer of ALPR information to other persons.
- (E) The title of the official custodian, or owner, of the ALPR system responsible for implementing this section.
- (F) A description of the reasonable measures that will be used to ensure the accuracy of the ALPR information and correct data errors.
- (G) The length of time ALPR information will be retained, and the process the ALPR operator will utilize to determine if and when to destroy retained ALPR information.

Cal. Civ. Code § 1798.90.51.

42. According to the ALPR Regulations, an ALPR end-user is required to:
- (a) Maintain reasonable security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure.
  - (b)(1) Implement a usage and privacy policy in order to ensure that the access, use, sharing, and dissemination of ALPR information is consistent with respect for individuals' privacy and civil liberties. The usage and privacy policy shall be available to the public in writing, and, if the ALPR end-user has an Internet Web site, the usage and privacy policy shall be posted conspicuously on that Internet Web site.
  - (2) The usage and privacy policy shall, at a minimum, include all of the following:
    - (A) The authorized purposes for accessing and using the ALPR information.
    - (B) A description of the job title or other designation or the employees and independent contractors who are authorized to access and use the ALPR information. The policy shall identify the training requirements necessary for those authorized employees and independent contractors.

- (C) A description of how the ALPR system will be monitored to ensure the security of the information accessed or used and compliance with applicable privacy laws and a process for periodic system audits.
- (D) The purposes of, process for, and restrictions on, the sale, sharing, or transfer of ALPR information to other persons.
- (E) The title of the official custodian, or owner, of the ALPR information responsible for implementing this section.
- (F) A description of the reasonable measures that will be used to ensure the accuracy of the ALPR information and correct data errors.
- (G) The length of time ALPR information will be retained, and the process the ALPR end-user will utilize to determine if and when to destroy retained ALPR information.

Cal. Civ. Code § 1798.90.53.

43. Pursuant to the ALPR Regulations, a “public agency shall not sell, share, or transfer ALPR information, except to another public agency, and only as otherwise permitted by law.” Cal. Civ. Code § 1798.90.55. However, “the provision of data hosting or towing services shall not be considered the sale, sharing, or transferring of ALPR information.” *Id.*

44. Pursuant to the ALPR Regulations, an individual who has been harmed by a violation of the ALPR Regulations may bring a civil action against a person who knowingly caused the harm, and the court may award a combination of any one or more of the following: (1) “[a]ctual damages, but not less than liquidated damages in the amount of two thousand five hundred dollars (\$2,500)”; (2) “[p]unitive damages upon proof of willful or reckless disregard of the law”; (3) “[r]easonable attorney’s fees and other litigation costs reasonably incurred”; and (4) “[o]ther preliminary and equitable relief as the court determines to be appropriate.” Cal. Civ. Code § 1798.90.54.

## ***Defendant's Violations of the ALPR Regulations***

### ***Defendant's Failures to Maintain Reasonable Security Procedures and Practices***

45. Defendant is, and at relevant times has been, an ALPR operator and ALPR end-user. As alleged herein, Defendant operates, and at relevant times has operated an ALPR system. Further, as alleged herein, Defendant accesses and uses, and at relevant times has accessed and used, its ALPR system for its own purposes.

46. In violation of the ALPR Regulations, at relevant times, Defendant failed to maintain reasonable security procedures and practices, including operational, administrative, technical and physical safeguards, to protect ALPR information from unauthorized access, destruction, use, modification and disclosure. *See* Cal. Civ. Code § 1798.90.51(a).

47. For instance, in violation of the ALPR Regulations, vulnerabilities in Defendant's ALPR system allowed attackers to tamper with a specified ALPR device and access sensitive information and credentials, among other things.

48. Further, in violation of the ALPR Regulations, certain of Defendant's ALPR cameras allowed people to view real-time footage and data from the cameras on the open internet without authentication.

49. Moreover, in violation of the ALPR Regulations, Defendant permitted end-users of its ALPR system to disclose ALPR information to unauthorized users and, at the same time, permitted unauthorized access and use of ALPR information.

50. For instance, in April 2026, it was reported in a news article that the UC Merced Police Department—an end-user of Defendant's ALPR system—was sharing ALPR information with numerous federal and non-California agencies, including Customs and Border Patrol –

National Targeting Center; (b) IRS Criminal Investigation; (c) United States Marshals Service; and (d) United States Secret Service.

51. An “Agency Data Sharing Report” prepared by Defendant and setting forth the agencies with which the UC Merced Police Department was sharing ALPR information confirmed the information reported in the news article.

52. The UC Merced Police Department was able to share the ALPR information with unauthorized agencies due to Defendant’s failure to maintain reasonable security procedures and practices, in violation of the ALPR Regulations.

53. Additionally, in April 2026, it was reported in a news article that the Merced, California Police Department—an end-user of Defendant’s ALPR system—was sharing ALPR information with numerous federal and non-California agencies, including the United States Marshals Service and the Bureau of Indian Affairs.

54. The Merced, California Police Department was able to share the ALPR information with unauthorized agencies due to Defendant’s failure to maintain reasonable security procedures and practices, in violation of the ALPR Regulations.

55. On information and belief, based on the Defendant’s history of security lapses, Defendant continues to fail to maintain reasonable security procedures and practices.

***Defendant’s Failure to Properly Implement and Post a Usage and Privacy Policy***

56. In violation of the ALPR Regulations, Defendant failed to: (a) implement a proper usage and privacy policy; and (b) post its usage and privacy policy conspicuously on its website.

57. For instance, in violation of the ALPR Regulations, Defendant’s usage and privacy policy does not include: (a) a “description of the job title or other designation of the employees and independent contractors who are authorized to use or access the ALPR system or to collect

ALPR information” (*see* Cal. Civ. Code § 1798.90.51(b)(2)(B)); or (b) a “description of the job title or other designation or the employees and independent contractors who are authorized to access and use the ALPR information” (*see* Cal. Civ. Code § 1798.90.53(b)(2)(B)).

58. Rather than including the requisite description of the job title or other designation, Defendant’s usage and privacy policy generically states that: (a) “[a]ll employees of the company are authorized to use the LPR system . . . .”; and (b) “[a]ll independent contractors of the company are authorized to use the LPR system . . . .”

59. Further, in violation of the ALPR Regulations, Defendant’s usage and privacy policy does not “contain a description of the reasonable measures that will be used to ensure the accuracy of the ALPR information and correct data errors.” *See* Cal. Civ. Code §§ 1798.90.51(b)(2)(F), 1798.90.53(b)(2)(F).

60. Rather than including the requisite description of the reasonable measures Defendant will use to ensure the accuracy of the ALPR information and correct data errors, Defendant’s usage and privacy policy merely states that its “collection of LPR data is automated so that the license plate images, and the details of when they are collected, are included in the system without review, along with the computer translation of the license plate number.”

61. Further, while Defendant’s usage and privacy policy acknowledges that its ALPR information may be incorrect, the policy does not describe how those errors will be corrected: “Although very infrequent, the license plate translation is sometimes inaccurate or incomplete. To avoid mistaken use of LPR data, the company recommends users of the data confirm the computer translation before taking any action as a result of LPR data.”

62. In further violation of the ALPR Regulations, Defendant has failed to conspicuously post its usage and privacy policy on its website, [motorolasolutions.com](http://motorolasolutions.com) (the

“Website”). *See* Cal. Civ. Code §§ 1798.90.51(b)(1), 1798.90.53(b)(1). Moreover, Defendant did not provide written public notice of its usage and privacy policy near each of its California ALPR Cameras.

63. Based on a review of the Website, the Website’s homepage does not contain a direct link to the relevant usage and privacy policy, nor does it otherwise reference or allude to the existence of any such policy.

64. Even if a Website visitor clicks on the “Products” link on the Website’s homepage and then further clicks on the links for “Video Security” and “License plate recognition,” the visitor is taken to a promotional page for Defendant’s ALPR system that, again, does not contain a direct link to the relevant usage and privacy policy, nor does it otherwise reference or allude to the existence of any such policy.

65. Moreover, even a Website visitor who affirmatively searches for “ALPR” or “automatic license plate recognition” using the Website’s search mechanism is not provided with a link to the relevant usage and privacy policy.

66. Far from being conspicuously posted on the Website, Defendant has buried the relevant usage and privacy policy at the following byzantine URL: [https://www.motorolasolutions.com/content/dam/msi/docs/products/license-plate-recognition-systems/reaperhd-mobile-lpr-system/lpr\\_usage\\_and\\_privacy\\_policy.pdf](https://www.motorolasolutions.com/content/dam/msi/docs/products/license-plate-recognition-systems/reaperhd-mobile-lpr-system/lpr_usage_and_privacy_policy.pdf).

***Plaintiffs’ Reasonable Expectation of Privacy and the Harm to Plaintiffs***

67. Based on publicly-available information, at relevant times, Defendant maintained, and continues to maintain, California ALPR Cameras near the UC Merced Entrance.

68. The California ALPR Cameras near the UC Merced Entrance indiscriminately capture license plate information, as well as the date, time and location, of all vehicles that pass by or park near the cameras.

69. Plaintiffs are residents of California that live in Merced, California. At relevant times, Plaintiffs travelled in their vehicles near the UC Merced Entrance.

70. For instance, at relevant times, Plaintiff Rojas travelled in her vehicle near and/or through the UC Merced Entrance on a near daily basis.

71. Among other times, Plaintiff Barriga travelled in her vehicle near and through the UC Merced Entrance on September 20, 2025 and March 12, 2026.

72. At relevant times, each time Plaintiffs travelled near and/or through the UC Merced Entrance—among other locations in California—unbeknownst to Plaintiffs and without their consent, Defendant’s California ALPR Cameras captured, *inter alia*, Plaintiffs’ personal information, including but not limited to their license plate numbers and geolocation data, as well as the date and time they travelled near or through the entrance.

73. Defendant did not provide written public notice of its usage and privacy policy anywhere near its California ALPR Cameras located near the UC Merced Entrance.

74. Defendant’s ALPR system provided the capability for Defendant and other users of the ALPR system to identify Plaintiffs as the drivers and/or registered owners of the vehicles they were driving.

75. At the time Defendant captured, *inter alia*, Plaintiffs’ license plate numbers, as well as the date, time and location of their vehicles, Defendant did not disclose to them the fact that it was doing so. Indeed, neither on the relevant California ALPR Cameras operated by Defendant

nor near them did Defendant disclose in writing the fact that its ALPR system was in use or any of the usage and privacy policy information required by the ALPR Regulations.

76. Because Defendant did not maintain reasonable security procedures and practices, at relevant times, when Plaintiffs travelled near or through the UC Merced Entrance, on information and belief based on the allegations contained herein, their information was unlawfully accessed and used by, and otherwise shared with and transferred to, various federal and out-of-state agencies.

77. At relevant times, Plaintiffs and Class members had a reasonable expectation that the dates, times and locations of their travels while in their personal vehicles would not be captured by Defendant's ALPR system and disclosed or otherwise shared with or transferred to the federal government and out-of-state public agencies in violation of California law.

78. Moreover, at relevant times, Plaintiffs and Class members had a reasonable expectation that their movements within their personal vehicles would not be tracked or capable of being tracked by the federal government and non-California public agencies via Defendant's network of California ALPR Cameras.

79. Based on recent reports of the federal government arresting United States citizens for seemingly lawful behavior, Defendant's failure to maintain reasonable security procedures and practices with respect to the ALPR information captured by its ALPR system has harmed Plaintiffs in the form of, *inter alia*, emotional distress and the fear that the federal government and non-California agencies are using the information about their travel and location in improper ways and for nefarious purposes.

80. Plaintiffs have suffered actual injury from having their personally identifiable information compromised by Defendant, including but not limited to: (a) violation of their right to

privacy; (b) the above-described emotional distress and fear; and (c) the imminent and impending injury arising from the unauthorized disclosure and use of the information captured by Defendant's ALPR system by the federal government and non-California agencies.

81. Defendant engaged in the unlawful conduct alleged herein knowingly, willfully and in reckless disregard of the law. Defendant knowingly caused the harm to Plaintiffs and Class members, as alleged herein.

### CLASS ACTION ALLEGATIONS

82. Plaintiffs bring this action, pursuant to 735 ILCS 5/2-801, individually and on behalf of the following Class: All individuals in the United States whose license plate number or other identifying information was captured by Defendant using Defendant's California ALPR Cameras during the class period.

83. Plaintiffs reserve the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery.

84. The "class period" is the time period beginning on the date established by the Court's determination of any applicable statute of limitations – after considering any tolling, concealment and accrual issues – and ending on the date of entry of any judgment.

85. Excluded from the Class are: (a) Defendant; (b) any parent, affiliate or subsidiary of Defendant; (c) any entity in which Defendant has a controlling interest; (d) any officers or directors of Defendant; (e) any successor or assign of Defendant; and (f) counsel for Plaintiffs and Defendant. Also excluded are any judge or court personnel assigned to this case and members of their immediate families.

86. **Numerosity:** The exact number of members of the Class is unknown and unavailable to Plaintiffs at this time, but individual joinder in this case is impracticable. The Class

likely consists of thousands of individuals, and the members can be identified through the records of Defendant and public records.

87. **Commonality and predominance:** Common questions of law and fact exist as to all Class members. These common questions of law and fact predominate over any questions affecting only individual members of the proposed Class. Common questions include, but are not limited to, the following:

a. Whether Defendant maintained reasonable security procedures and practices, including operational, administrative, technical and physical safeguards to protect Plaintiffs' and Class members' ALPR information from unauthorized access, use, modification and disclosure;

b. Whether Defendant implemented a usage and privacy policy that was available to the public in writing and conspicuously posted on its Website;

c. Whether Defendant implemented a usage and privacy policy that contained the information required by the ALPR Regulations;

d. Whether Defendant's conduct violated the ALPR Regulations; and

e. Whether Plaintiffs and Class members have been harmed and the proper measure of relief.

88. **Typicality:** Plaintiffs' claims are typical of the claims of the Class they seek to represent. The claims of Plaintiffs and Class members arise from the same conduct by Defendant and are based on the same legal theories.

89. **Superiority:** Absent a class action, most Class members would find the cost of litigating their claims to be prohibitively expensive and would thus have no effective remedy. The class treatment of common questions of law and fact is superior to multiple individual actions or

piecemeal litigation in that it conserves the resources of the courts and the litigants and promotes consistency and efficiency of adjudication. Further, certification of a class action to resolve this matter will reduce the possibility of repetitious litigation involving potentially thousands of class members.

90. **Adequacy:** Plaintiffs will fairly and adequately represent and protect the interests of the Class in that they have no interest that is antagonistic to, or that irreconcilably conflicts with, those of other Class members. Further, Plaintiffs have retained counsel competent and experienced in the prosecution of class action litigation.

### **CLAIM FOR RELIEF**

#### **COUNT ONE** **VIOLATION OF CALIFORNIA CIVIL CODE § 1798.90.5, *et seq.***

91. Plaintiffs restate and reallege the allegations of paragraphs 1 through 90, above, as though fully set forth herein.

92. Plaintiffs bring this Count against Defendant individually and on behalf of members of the Class.

93. Each Plaintiff is a natural person and thus, an “individual” pursuant to Cal. Civ. Code § 1798.90.54(a).

94. Defendant is a “person” pursuant to Cal. Civ. Code § 1798.90.5(e) because it is a corporation.

95. As alleged herein, Defendant is an: (a) ALPR operator because it operated and continues to operate an ALPR system; and (b) ALPR end-user because it accessed and used, and continues to access and use, an ALPR system.

96. As alleged herein, Defendant violated the ALPR Regulations by failing to maintain reasonable security procedures and practices.

97. As alleged herein, Defendant violated the ALPR Regulations by failing to have a usage and privacy policy that was posted conspicuously on its Website.

98. As alleged herein, Defendant violated the ALPR Regulations by failing to have a usage and privacy policy that contained the minimum information required by the ALPR Regulations.

99. As alleged herein, Defendant knowingly caused harm to Plaintiffs and Class members via its violations of the ALPR Regulations. As such, Plaintiffs are entitled to bring this action and are further entitled to: (a) actual damages in an amount not less than liquidated damages of \$2,500; (b) punitive damages; (c) reasonable attorney's fees and other litigation costs reasonably incurred; and (d) preliminary and equitable relief as the Court determines to be appropriate.

WHEREFORE, Plaintiffs, on behalf of themselves and members of the Class respectfully requests that the Court:

- a. Certify the proposed Class, name Plaintiffs the representatives of the proposed Class and appoint Plaintiffs' counsel as Class counsel;
- b. Award each Plaintiff and each member of the proposed Class actual damages in an amount not less than liquidated damages in the amount of \$2,500, punitive damages and any other type of permissible damages in amounts to be determined at trial;
- c. Grant preliminary and permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts and practices alleged herein;
- d. Enter an order declaring that Defendant violated the statutory provisions alleged herein;

- e. Award Plaintiffs and members of the proposed Class pre-judgment and post-judgment interest as permitted by law;
- f. Award to Plaintiffs their reasonable attorney's fees and other litigation costs reasonably incurred; and
- g. Grant all such other relief as it deems just and proper.

**JURY DEMAND**

Plaintiffs demand a trial by jury on all causes of action and issues so triable.

Dated: May 27, 2026

Respectfully submitted,

Michelle Rojas and Marissa Barriga,  
individually and on behalf of all other persons  
similarly situated,

By: /s/ Scott R. Drury  
SCOTT R. DRURY  
*One of Plaintiffs' Attorneys*

Scott R. Drury  
DRURY LEGAL, LLC  
6 Carriage Lane  
Highwood, Illinois 60040  
(312) 358-8225  
scott@drurylegal.com  
Firm ID No.: 100500

Joshua D. Arisohn (to be admitted *pro hac vice*)  
ARISOHN LLC  
94 Blakeslee Rd.  
Litchfield, CT 06759  
(646) 837-7150  
josh@arisohnllc.com

*Counsel for Plaintiffs and Putative Class Members*

# ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Class Action Lawsuit Claims Motorola Solutions License Plate Readers Violate California Privacy Laws](#)

---