MITCHELL CHYETTE [113087]
Law Office of Mitchell Chyette
125 12th Street
Suite 100-BALI
Oakland, CA 94607
Telephone: (510) 388-3748
Email: mitch@chyettelaw.com
Attorney for Petitioners

IN THE SUPERIOR COURT OF CALIFORNIA

COUNTY OF ALAMEDA

SECURE JUSTICE, INC., a California non-profit organization, and BRIAN HOFER, a California citizen Petitioners, vs THE CITY OF OAKLAND, Oakland.	Case No. RG **PETITION FOR WRIT OF MANDATE AND PROHIBITION**

I. INTRODUCTION

1. Yogi Berra once observed, "It's déjà vu, all over again." Sadly, the parties have been here before, quite recently.

2. On September 2, 2021, Petitioners sued The City of Oakland (Case No. RG1111681) over some of the same misconduct identified below, including the unlawful sharing of license plate data in violation of SB 34 ((Hill) (Civil Code § 1798.90.5 et seq.) and Oakland's own ordinance, and the unlawful sharing of ShotSpotter data with unapproved third parties in violation of Oakland's ordinance.

3. The parties supposedly settled the matter at mediation in October 2023. In January 2024, the City Council adopted the settlement agreement, attached as **Exhibit A** ("Settlement Agreement").[1] Oakland has been in breach of the Settlement Agreement ever since.

4. Among other things, Oakland promised to refrain from further violating SB 34, a state law regulating the use of automated license plate readers ("ALPR"), and to comply with the current version of Departmental General Order ("DGO") I-12 (the police department's use policy for ALPR, created to comply with both SB 34 and Oakland's Surveillance Technology Ordinance codified in the Oakland Municipal Code ("O.M.C.") at Chapter 9.64 et seq. ("Surveillance Ordinance")). A copy of the operative DGO I-12 is attached as **Exhibit B**. A copy of the Surveillance Ordinance is attached as **Exhibit C**.

5. DGO I-12 was approved in August 2024. Oakland has been in violation of it since then.

6. SB 34 was enacted on January 1, 2016. For all but seven months of the law's 10-year existence, during which Oakland had no license plate readers, Oakland has violated SB 34.

[1] There was a minor amendment made subsequent to adoption that is not relevant to the instant action, thus it is not included.

7. At the October and November 2025 meetings of the Privacy Advisory Commission ("PAC"), Oakland produced a required annual report for its Crime Tracer technology— essentially a "Google" search tool that aggregates data from many systems, allowing for faster queries. As described more fully below, during the upfront approval process, Oakland stated in both the analysis statement and the enforceable use policy DGO I-24 that Oakland's ALPR data would *not be made* accessible to anyone but the Oakland Police Department ("OPD") due to privacy concerns. A copy of DGO I-24 is attached as **Exhibit D**. The annual report revealed, however, that ALPR data *was made* accessible, and Oakland admitted that at least six federal agencies and a significant number of non-California state or local agencies, from deep red states that prosecute immigration, reproductive choice and gender affirming care, had access to Oakland's ALPR data via the Crime Tracer platform, where millions of queries are performed. A copy of the 2024 Crime Tracer Annual Report is attached as **Exhibit E**.

8. The data sharing prohibition of SB 34 is not limited to any particular ALPR platform, portal, or vendor. By illegally sharing data with ineligible agencies, Oakland is violating SB 34 via both its Flock Safety ALPR sharing portal and via Crime Tracer.

9. By illegally sharing tens of millions of sensitive location data points from millions of individuals *each month* since August 2024, Oakland has exposed countless individuals to grave harm from the Trump Administration's hate-filled policies and invaded the privacy rights of individuals not suspected of any wrongdoing. There could also be a negative impact on criminal investigations whose integrity are called into question because of these due process violations.

10. In addition, Oakland has violated its own competitive bidding rules by illegally issuing sole-source contracts for both ShotSpotter and Flock Safety ALPR, causing harm to taxpayers by obligating Oakland to pay millions more than comparable vendors are charging for the same technologies.

11. Despite obvious violations of SB-34, the Surveillance Ordinance, and DGO I-24, in two separate annual reports (Crime Tracer and Flock Safety ALPR discussed below), OPD stated that it was *unaware* of any policy violations, calling into question the entire integrity of this framework and whether any representations by OPD can be believed.

12. The subsequent harm at issue here is greater than the previous lawsuit because Oakland is continuing its same unlawful practices even after being sued, despite recent negative media exposure, threats of litigation for the new violations, and the grave harm posed to Oakland residents by the Trump Administration's war on sanctuary cities like Oakland. Petitioners seek the most aggressive relief the Court can provide, including but not limited to terminating the use of these technologies.

II. JURISDICTION AND VENUE

13. This Court has jurisdiction under the California Constitution, Article VI, section 10, and Code of Civil Procedure sections 1085 and 1060.

14. Venue in this Court is proper because Petitioners' claims arose in Oakland, and because this is an action against an Oakland agency. Code Civ. Proc. § 394.

III. PARTIES

15. Petitioner Secure Justice, Inc. ("Secure Justice") is an IRS-registered non-profit organization located in Oakland, Alameda County, that advocates against state abuse of power and for a reduction in government and corporate overreach.

16. Petitioner Brian Hofer ("Hofer") is an individual resident of Alameda County, executive director, and chair of the board of Secure Justice.

17. Petitioners have been assessed and paid taxes in the jurisdiction within the past year.

18. Respondent the City of Oakland is a charter city of the State of California. The Oakland Police Department ("OPD") and Oakland Attorney ("OCA") are Oakland departments. Oakland Staff are employees of Oakland.

19. Secure Justice and Mr. Hofer are real parties in interest in this action. Residents of California are guaranteed a right to privacy under California Constitution, Article I, section 1. As a resident and near-daily driver in Oakland, Petitioner Hofer has a vital interest in seeing that the OPD's use of police surveillance technology does not infringe upon that right. Secure Justice is a "representative organization,"

20. Petitioners have no legal remedy that would compel Oakland to do its duty under the laws discussed below.

IV. A WRIT OF MANDATE/PROHIBITION IS NECESSARY AND APPROPRIATE

FIRST CAUSE OF ACTION

(Against Oakland)

Failure to Perform Mandatory Duties Under Civil Code section 1798.90.5 *et seq* ("SB 34"), and Violations of O.M.C. 9.64. *et seq.* ("Surveillance Ordinance") regarding Automated License Plate Readers

21. Petitioners incorporate by reference the allegations of the above paragraphs as though fully set forth herein.

22. OPD uses a mass surveillance technology called automated license plate reader ("ALPR"). This technology allows an OPD officer to use a camera to scan a scene, from which the computer software's artificial intelligence (AI) will identify all license plate numbers. The AI can then inform the police officer of any information OPD has in any other databases relating to the car or the owner. In addition, the AI coordinates with GPS, so that the AI can record where and when the car was seen. The collection of such data is indiscriminate, identifying all drivers that pass in view of the camera. Historically, less than 0.1% of the scanned plates will ever be used for investigatory purposes.

23. In 2016, pursuant to state law SB 34, OPD drafted the mandated policy for using ALPR and ALPR data. A copy of SB 34 is attached as **Exhibit F**.

24. On February 13, 2020, the California State Auditor published a review of four agencies pertaining to the use of ALPR technology, and found them grossly noncompliant with SB 34, including by sharing ALPR information with out-of-state and federal agencies, and lacking sufficient guardrails to protect the sensitive data. A copy of the audit is attached as **Exhibit G**.

Non-Compliance with Civil Code section 1798.90.5 *et seq*—Sharing Data with Ineligible Agencies.

25. SB 34 narrowly restricts sharing ALPR information. Civ. Code, § 1798.90.52(b). A user of ALPR may only share data with a "public agency." SB 34 states that a "public agency shall not sell, share, or transfer ALPR information, except to another public agency, and only as otherwise permitted by law." Civ. Code, §1798.90.55(b). Civ. Code, §1798.90.5(f). "Public agency" means a California state agency; it excludes out-of-state or federal agencies.

26. On September 2, 2021, after years of warning Oakland that it was violating SB 34, Petitioners filed a petition for writ of mandate and prohibition in this court, Case No. RG 21111681, seeking a writ of mandate and/or prohibition to force Oakland to comply with SB 34.

27. On October 27, 2023, the California Department of Justice issued Bulletin 2023-DLE-06, reminding California law enforcement agencies of SB 34's prohibition on sharing ALPR information with out-of-state or federal agencies, their obligation to ensure that adequate safeguards were in place, and to maintain a record of access. A copy of the bulletin is attached as **Exhibit H**.

28. On January 4, 2024, Oakland adopted the Settlement Agreement of the parties, which, among other things, included a promise by Oakland to comply with DGO I-12, which, in turn, incorporates SB 34.

29. Oakland honored SB 34 and the Settlement Agreement for several months, only because they had no ALPR technology, having abandoned their older mobile readers.

30. In August 2024, upon adoption of revised DGO I-12, Oakland began operating a new ALPR system from Flock Safety, the dominant provider of ALPR technology to municipalities.

31. Also in August 2024, OPD immediately began to violate SB 34, the Surveillance Ordinance, and DGO I-12 again by providing ALPR information to federal agencies, and by allowing unfettered access to many third parties—some of whom provided the information to Immigration and Customs Enforcement ("ICE"), in violation of California and Oakland's sanctuary status.[2]

32. Petitioners obtained the Flock Safety Network Audit of the OPD ALPR system, which captures third-party access, and the Flock Safety Organizational Audit, which tracks OPD's own queries, through a public records act request. The documents revealed that OPD provided ALPR information to federal agencies. In addition to previous quoted sections, DGO I-12 plainly states that "Data may not be shared with out-of-state or federal agencies, per California law." DGO I-12 Section G. Data Access. OPD's July 16, 2024, staff report to the City Council restates this prohibition on data sharing, confirming OPD's awareness of the law.

33. On October 3, 2025, the California Attorney General sued El Cajon (San Diego County) for violating the SB 34 data sharing prohibition at issue here.

34. OPD is authorized to operate 290 ALPR readers. Per the April 2025 annual report, OPD collects on average 48 million plate scans per month. Its third-party access logs revealed that millions of searches by external agencies have occurred.

---

[2] "The logs show that since installing hundreds of plate readers last year, the departments have shared data for investigations related to seven federal agencies, including the FBI. In at least one case, the Oakland Police Department fulfilled a request related to an Immigration and Customs Enforcement investigation." https://sfstandard.com/2025/07/14/oakland-san-francisco-ice-license-plate-readers/

35. A review of the audits also reveals that OPD further violated SB 34 and DGO I-12 by allowing use of its data by third parties who then shared it with federal and out-of-state agencies, thereby failing to maintain adequate guardrails. Various entries in these audits reference searches performed for federal agencies like ICE, HSI, FBI, DEA, FBI JTTF, ATF, USMS, and USPS. OPD had been warned by Petitioner Hofer for years about the risk from third-party proxy searches, yet OPD took no reasonable measures to safeguard the data, as mandated by SB 34.[3] Many of the above federal agencies have been repurposed to facilitate civil immigration deportation efforts, at the direction of the Trump administration.

36. Per Flock Safety ALPR materials, the system offers multiple sharing arrangements, including "National Lookup," where all Flock Safety customers in the country get unfettered direct access to the data of all customers that have opted in; "Statewide Lookup" (unfettered direct access for opted-in partners in the respective home state of the customer), by specific region (e.g. nearby counties), and direct 1:1 sharing, wherein a customer like OPD would add agencies one by one.

37. OPD is aware of Oakland's Sanctuary City ordinance, its Sanctuary Contracting Ordinance (which prohibits the award of contracts to vendors that provide data to ICE, as Flock Safety has done), and California's SB 34 and 54, the latter of which prohibits the use of municipal resources to aid in federal immigration enforcement efforts.

38. Despite years of a fairly static third-party sharing protocol in DGO I-12, and despite having been sued before for violating SB 34, and despite the plain language of the mostly-drafted-by-OPD DGO I-12 operative policy approved August 2024, which clearly requires case-by-case approval of all third party requests for data as it has for years, OPD unilaterally chose to ignore all the guardrails imposed by SB 34 and DGO I-12 and instead allowed unfettered direct access to a

[3] OPD and the Privacy Advisory Commission were in discussions over third-party proxy concerns pertaining to a new Flock Safety CCTV camera proposal from OPD at the time the SF Standard story broke (Footnote 2, *supra*).

continuously-growing list of agencies. Although this may have reduced the administrative burden on OPD of reviewing requests for data, it has eviscerated the intent of the guardrails created by SB 34 and DGO I-12 to guard against the very horror stories we have seen occurring with greater frequency in the news, as the Trump administration and red states target marginalized communities quite often by using data harvested from surveillance technology.

39. By enabling unfettered direct access, OPD can no longer ensure that prior to the data being accessed a requesting agency has the right to know and need to know, and that they have entered the SB 34/DGO I-12 mandated search criteria—including the very important (and often lacking from the Flock Safety Network Audit records) "purpose" of the search to ensure that it complies with DGO I-12's authorized uses.

40. Today, when a requesting agency like the San Francisco Police Department searches for a particular plate number, the Flock Safety portal searches all networked partners that have added San Francisco, which includes Oakland. OPD has no idea its data is being searched and does not know in real time the reason(s) why. It is only after running an audit, long after the sensitive location data has been revealed, that OPD learns which agency requested data, and depending on compliance, the who, what, when, where, and why mandated by SB 34, which requires that a record of access capturing this query info be maintained. It is impossible for them to comply with SB 34 and DGO I-12 in this manner.

41. OPD also provides unfettered direct access to its ALPR data to the San Francisco federal fusion center Northern California Intelligence Regional Center ("NCRIC"). Federal agents from the ATF, DEA, FBI, IRS, USMS, USPS, DHS, and USFS are hosted at NCRIC and have access to its databases, with the goal of such a fusion center being to commingle data and share information between federal and local agencies. By providing unfettered direct access to NCRIC, OPD cannot ensure that there are reasonable guardrails in place sufficient to protect its data and comply with SB 34 and DGO I-12.

42. As stated by California Attorney General Rob Bonta in his press release announcing the action against El Cajon: "When information about Californians leaves the state, we no longer have any say over how it is used or shared. That is why the California Legislature passed SB 34— to ensure information about Californians remains here in California. Yet El Cajon has knowingly and repeatedly refused to comply with state law, jeopardizing the privacy and safety of individuals in its community."[4] Oakland has done the same, willfully ignoring the state-mandated guardrails needed to protect this sensitive data.

43. OPD has a mandatory duty to protect the integrity of the data collected and to refrain from data sharing with federal or out-of-state agencies. Per SB 34, an ALPR operator is defined as one that operates an ALPR system. Civ. Code, §1798.90.5(c). An ALPR end-user is defined as one that accesses or uses an ALPR system. Civ. Code, §1798.90.5(a).

44. Among other things, an ALPR operator like OPD has a mandatory duty to "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, and implement a usage and privacy policy which proscribes the rules of use, including the specific authorized purposes for using the system and collecting data." Civ. Code, §1798.90.51.

45. If an ALPR operator accesses, or provides access, to ALPR information, the operator has a mandatory duty to maintain a record of that access. At a minimum, the record must include the date and time the information was accessed, the license plate number or other data elements used to query the system, the username of the person who accessed the information and the organization they are affiliated with, and critically, the purpose for accessing the information. Civ Code, §1798.90.52. As the California State Auditor found, SB 34 was being violated

[4] https://oag.ca.gov/news/press-releases/attorney-general-bonta-sues-el-cajon-illegally-sharing-license-plate-data-out

statewide by police agencies that allowed open-ended fishing expeditions of its data, in violation of the law and infringing upon our right to privacy.

46. An ALPR end-user like OPD has a similar duty as an operator, to maintain appropriate guardrails, and to implement a usage and privacy policy. Civ Code, §1798.90.53.

47. OPD's DGO I-12 places further obligations on OPD in addition to the obligations imposed by SB 34. DGO I-12 requires a multi-step approval process for agencies requesting ALPR information when there is no legal obligation by OPD to provide it.

48. The policy requires that the requesting party have a right to know (such as being a sworn law enforcement officer) and a need to know (such as being the investigating officer). DGO I-12 requires that the requesting party's name, right, and need to know be documented, and further requires that OPD record whether the request was honored or denied, the reason for such action, and the name of the OPD officer who processed the request.

49. From the first day it went into effect, no part of the DGO I-12 third-party request protocol was honored, resulting in millions of violations of the policy and SB 34. Petitioner Hofer has been informed by OPD that, despite the negative media attention and litigation threat, OPD has not changed any of its ALPR practices in an attempt to mitigate the harm OPD has caused. Millions of sensitive location data points are illegally accessed and shared each day.

50. In response to the obligation regarding results of internal audits or information about policy violations, OPD stated in its Annual Report that they were not aware of any violations or potential violations of DGO I-12.

51. When OPD made the above statement, they knew it was false. Their own records reveal that OPD illegally shared ALPR information with federal agencies, in violation of SB 34 and DGO I-12.

52. OPD's internal records and practices also revealed that DGO I-12's case-by-case approval process for third-party data requests had never been adhered

to. Instead, OPD provided unfettered access to its data to networked partners that also use Flock Safety, in violation of SB 34, DGO I-12, the Surveillance Ordinance, and the Settlement Agreement.

53. Beginning with the 2016 SB 34 obligation to create a use policy for ALPR, Oakland has had several versions of DGO I-12 to date, with the operative version approved in August 2024 (Exhibit B). Although several provisions have been modified over time, the third-party data sharing protocol has not substantively changed.

54. For years, OPD has known that third-party requests must meet certain criteria before sharing, and that unfettered access would clearly be illegal.

55. By using the Flock Safety ALPR system in an unapproved manner every day, each day of use has violated O.M.C. 9.64.030 1 C, by using surveillance technology for a purpose or manner not previously approved by the City Council pursuant to the Surveillance Ordinance requirements.

56. For all entities that might request data from OPD, Section K is split into two parts: one where a legal order, such as a warrant or subpoena, applies, and two for requests lacking such an order. The language is clear for those lacking a legal obligation, that requests shall be made in writing and only approved per the protocol outlined in the section. DGO I-12 also makes clear that server "access shall be restricted only to authorized/designated OPD personnel who will extract the required information and forward it to the requester."

57. DGO I-12 requires OPD to confirm that a requesting party has both a right to know, and a need to know, such as direct involvement in an investigation (to prevent fishing expeditions), that OPD must record the requestor's name, document, and the right and need to know, and that OPD must record whether the request was honored or denied, the reason why, and the name of the approving officer.

58. SB 34 further requires OPD to maintain a record of access that also captures the date and time the information was accessed, the license plate number

or other data elements used to query, the username of the person who accessed the information and their organizational affiliation, the purpose for accessing the information, and that any ALPR information only be used according to the authorized purposes in the host's own use policy, here DGO I-12. Civ. Code, §1798.90.52. The above protocols are not being followed and have never been followed in full under the August 2024 operative policy.

59. DGO I-12, section K, mandates that third-party search requests shall be maintained, so that information about these requests can be shared in the required annual report. The third-party requests were not provided with the 2024 annual report.

60. DGO I-12, section M, mandates that the records of Database Investigatory Queries, Third-Party Data Sharing, and Hot List entries be incorporated into the annual report. Neither the Third-Party Data Sharing nor Hot List entries were provided with the 2024 Annual Report.

61. Petitioners became aware of these unfavorable-to-OPD documents after the SF Standard story referenced in footnote 1 above. The SF Standard obtained the documents via a public records request to Oakland.

62. By withholding from the Privacy Advisory Commission, City Council, and the general public, these documents which revealed an enormous number of violations of state law and DGO I-12, and by certifying that no policy violations had occurred in the past year, OPD intentionally presented a false rosy picture when seeking necessary approval during the annual review for ongoing use to be authorized under O.M.C. 9.64.040 2.

Compliance with the Civil Code section 1798.90.5 *et seq*—Prohibition on Data Sharing Against Policy

63. SB 34 places additional obligations on OPD, allowing third-party access to OPD's ALPR information "only for the authorized purposes described in…" OPD's own use policy, DGO I-12. Civ. Code, §1798.90.52(b).

64. Like SB 34, the Surveillance Ordinance requires that the ALPR use policy describe the specific authorized uses for the technology. Civ. Code, §1798.90.51(b)(2)(A), and O.M.C. 9.64.010 16 B.

65. DGO I-12 states that historical searches of scanned plates are "permissible solely for [searching for] missing or at-risk persons, witness locates, burglaries, grand theft, violent crime investigation, and in response to any subpoena warrant, or other court order." DGO I-12 Section D-2 Authorized Use – Database Investigative Queries. This same section further restates the obligation on OPD to maintain the record of access required by SB 34.

66. OPD violated SB 34 and DGO I-12 by allowing searches outside the scope of these authorized uses and any recognizable specific authorized use at all (e.g., "intel," "search," or a case number without any stated purpose). Without this category of information, it is impossible to ascertain whether these additional searches were done for legitimate or illegitimate purposes, and they defeat the intent of DGO I-12's third-party data sharing guardrails, and SB 34's record of access requirement.

Failure to Maintain Reasonable Security Procedures and Practices to Protect ALPR information from Unauthorized Access, Destruction, Use, Modification, or Disclosure.

67. During the relevant time period, OPD knew that the Trump Administration had publicly attacked Oakland's sanctuary status.[5] OPD also knew that Flock Safety's ALPR network had received significant negative media attention after several municipalities in Illinois and Colorado terminated their relationships upon discovering that Flock Safety had provided direct access to federal immigration agencies without their local customers' knowledge, and then lied about it when exposed.[6]

[5] https://oaklandside.org/2025/05/02/trump-sanctuary-cities-executive-order-federal-funding/

[6] https://abc7chicago.com/post/evanston-oak-park-end-contracts-Flock Safety-safety-license-plate-reader-company-investigation-illinois/17678137/

68. By July 2024, prior to DGO I-12 becoming operative, Petitioner Hofer had informed OPD that many California police departments openly defied SB 34's data sharing prohibition, and Attorney General Bonta's guidance memo restating the same.[7] Others, like Riverside County Sheriff Chad Bianco, proclaimed they opposed both SB 34 and SB 54, the California Values Act, which generally prohibits the use of local resources in immigration enforcement actions.[8]

69. Petitioner Hofer forwarded to OPD specific media reports and quotes from agencies like Oakley, Brentwood, Antioch, and Riverside demonstrating their public refusal to comply with SB 34.

70. During this relevant time period, the media and Petitioner Hofer alerted OPD to Flock Safety's decision to use stolen data obtained from the dark web in its new Nova product.[9]

71. At the October 2, 2025, Privacy Advisory Commission hearing, a commissioner informed OPD about Flock Safety's illegally re-installing its readers after being ordered to remove them by Evanston, Illinois.[10]

72. Despite all the news coverage, Petitioner's original lawsuit over some of the same misconduct here, and knowledge of their own unlawful actions, OPD continued to move forward and did not consider any of these reports to be red flags, showing a careless and unreasonable disregard for the data privacy rights of Oaklanders and those visiting or commuting through. OPD continues to provide unfettered access to its data.

---

[7] https://www.newsweek.com/california-sharing-license-plate-data-anti-abortion-states-1882974

[8] https://www.calonews.com/communities/riverside-sheriff-bianco-joins-far-right-legal-group-seeking-to-end-sanctuary-laws-in-california/article_cbc7bac9-2e7f-455f-8693-5f4a00022731.html

[9] https://www.404media.co/license-plate-reader-company-Flock Safety-is-building-a-massive-people-lookup-tool-leak-shows/

[10] https://evanstonroundtable.com/2025/09/24/Flock Safety-safety-reinstalls-evanston-cameras/

73. Because OPD has repeatedly and intentionally failed to adhere to SB 34 as alleged herein, in that they failed to maintain appropriate guardrails as required despite knowledge of the obvious risks and awareness of their own previous misconduct, because OPD has been sued before by Petitioners for this very misconduct, because OPD violated its Settlement Agreement with Petitioners pertaining to this very issue, because OPD violated O.M.C. 9.64.030 1 C. (using existing surveillance technology or the information it provides for a purpose, in a manner…not previously approved by the Oakland Council pursuant to the Ordinance and its corresponding use policy, Petitioners request that this Court issue a writ of prohibition terminating the Respondent's use of ALPR technology.

WHEREFORE, as existing state law, Oakland policy, and previous litigation have been insufficient to prevent OPD's misconduct, and because Oakland violated its Settlement Agreement with Petitioners, Petitioners request that the Court issue a writ of prohibition requiring the following:

A. That Oakland be prohibited from using ALPR.

B. That Petitioners' attorney's fees and court costs be awarded per Civ. Code, §1798.90.54 and O.M.C. 9.64.050.

SECOND CAUSE OF ACTION

(Against Oakland)

Breach of Settlement Agreement

74. Petitioners incorporate by reference the allegations of the above paragraphs as though fully set forth herein.

75. As alleged herein, Oakland breached the Settlement Agreement Section 4 B, in that it failed to adhere to SB 34 and DGO I-12.

WHEREFORE, as existing state law, Oakland policy, and prior litigation have been insufficient to prevent OPD's misconduct, and because Oakland violated its settlement agreement with Petitioners, Petitioners request that the Court issue a writ of prohibition requiring the following:

A. That Oakland be prohibited from using ALPR.

B. That Petitioners' attorney's fees and court costs be awarded per Civ. Code, §1798.90.54 and O.M.C. 9.64.050.

THIRD CAUSE OF ACTION

(Against Oakland)

Failure to Produce Documents Under the Public Records Act

76. Petitioners incorporate by reference the allegations of the above paragraphs as though fully set forth herein.

77. On April 23, 2024, Petitioners submitted a request for public records pertaining to Oakland's use of ShotSpotter, a gunshot-detecting technology.

78. Petitioners requested OPD call logs for the 199 cases referenced in an April 2024 ShotSpotter annual report produced under the Surveillance Ordinance. Petitioners further requested any documents referencing first aid and/or medical care that was provided during the 199 cases. (Request No. 24-4633).

79. On April 24, 2024, Oakland responded to the request, stating: "Unknown until the query is conducted for disclosure." To date, Oakland has provided no further response.

80. OPD failed to produce any of the documents it has in response to Public Records requests 24-4633.

81. OPD has a mandatory duty to produce all responsive documents under the Public Records Act, Govt. Code section 7290 et seq.

WHEREFORE, Petitioners request that the Court issue a writ of mandate compelling the Oakland to fulfill the requirements of the Public Records Act concerning the requests identified, and that Petitioners' attorney's fees and court costs be awarded per Gov. Code, §7923.115.

FOURTH CAUSE OF ACTION

(Against Oakland)

Violations of Purchasing Ordinance—OMC 2.040 et seq.

82. Petitioners incorporate by reference the allegations of the above paragraphs as though fully set forth herein.

83. In the alternative, without conceding that ShotSpotter-like technology is ever effective or cost-efficient, in addition to the above misconduct, OPD misled the City Council to obtain a competitive bidding waiver for ShotSpotter.

84. OPD is presently attempting to seek a similar competitive bidding waiver for its proposed Flock Safety citywide mass surveillance system, to include Flock Safety ALPR, Flock Safety Closed Circuit Television cameras ("CCTV"), and Flock Safety OS, the "brain" to run its real-time crime center.

85. In past staff reports seeking approval to enter into or renew a contract for ShotSpotter, OPD misled the City Council by falsely claiming that ShotSpotter has been approved, endorsed, or scientifically validated as to efficacy by the U.S. Department of Justice.

86. OPD further misled the City Council by falsely claiming that only ShotSpotter can provide the desired services, despite knowing that multiple vendors provide similar technology, including Flock Safety, with whom OPD has an existing relationship.

87. Both ShotSpotter and Flock Safety provide quotes based on the square mileage of coverage area for their respective gunshot detection technology. Flock Safety's Raven gunshot detecting technology is 50% cheaper than ShotSpotter's contract rate with Oakland. As of October 2024, when the ShotSpotter contract proposal was presented to the City Council, ShotSpotter cost Oakland $73,500 per square mile of coverage. At that time, Flock Safety charged $35,000 per square mile of coverage. At these prices, switching to Flock Safety would have saved Oakland $1.5 million over the three-year contract term that was given to ShotSpotter.

88. As OPD presently uses Flock Safety and clearly desires to incorporate its various technologies and data streams into a centralized platform called Flock Safety OS, it would have made more sense for OPD to choose Flock Safety's Raven product at 50% of the cost of ShotSpotter.

89. When Petitioner Hofer, who was aware that the ShotSpotter contract had expired, asked OPD's Flock Safety sales representative why they had never bid

on the gunshot detecting technology, the representative replied, "Because Oakland hasn't put it out to bid."

90. Oakland's purchasing ordinance requires that for any service that exceeds $50,000, Oakland shall call for formal bids by advertising. O.M.C. 2.04.050 A. As Oakland's current contract with ShotSpotter exceeds $2 million, it should have been sent out for competitive bid.

91. OPD knew it was deceiving the City Council and harming the taxpayers when they presented this false information in pursuit of the ShotSpotter contract.

92. For the past two years, and for the foreseeable future, Oakland's financial outlook is precarious. Paying double the price for the same technology harms the taxpayers of Oakland at a time when Oakland can ill afford to overpay.

93. During the course of the late summer and early fall meetings between OPD and the Privacy Advisory Commission, several commissioners asked OPD about alternate vendors as it became clear that the majority of commissioners were concerned about OPD's preferred vendor's reputation, which was rapidly falling apart in the national news media.

94. A representative for OPD repeatedly stated that "other vendors would have the same problems," but could not identify what they were. As the same commissioner pressed him as to how OPD could know for certain that no other vendor could compete when OPD had not even bothered to ask, OPD finally admitted they did not know.

95. In addition to potentially missing out on more competitive pricing, a competitor's bid might have revealed better privacy guardrails or operational security than Flock Safety offers. Aside from Vigilant Solutions, Petitioners are unaware of any other major ALPR vendor that provides data to ICE, as Flock Safety has done.

96. Awarding a no-bid contract to Flock Safety for ALPR, CCTV, and Flock OS, would harm Oakland taxpayers by overpaying, and by providing data to ICE,

and lying about it, would violate at least the spirit of SB 54, Oakland's Sanctuary City Ordinance, and Oakland's Sanctuary Contracting Ordinance, if not the actual letter of these laws.

97. Petitioner Hofer has a decade of experience as a subject matter expert in this area. He is aware of many CCTV vendors that could compete on the regular camera portion of the contract, and a half dozen ALPR vendors that can compete with Flock Safety on price point and features offered, and that do not provide data to federal immigration agencies.

WHEREFORE, Petitioners pray for a writ of mandate requiring OPD to seek competitive bidding for all surveillance technologies, including ShotSpotter and ALPR, because Oakland violated its competitive bidding obligations and harmed Oakland taxpayers.

ADDITIONAL PRAYER FOR RELIEF

WHEREFORE, Petitioners request that this Court:

A. Issue a writ of mandate and/or prohibition as specified above;

B. Award Petitioners their attorney's fees and costs as provided by the Surveillance Ordinance, SB 34, Public Records Act, and Civ. Code, §1021.5;

C. Order such other relief as the Court deems just.

Date: November 17, 2025

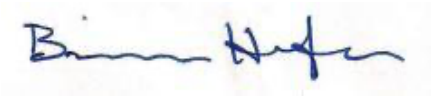
Law Office of Mitchell Chyette

Mitchell Chyette
Attorney for Petitioners Secure Justice, and Brian Hofer

VERIFICATION

I, Brian Hofer, am one of the Petitioners in this action and I am the Chair of the Board and Executive Director of Secure Justice, Inc. I am authorized to execute this verification on its behalf. I have read the foregoing Petition for Writ of Mandate or Prohibition, and I hereby verify that based on my personal knowledge, the facts alleged are true.

Executed this 17th day of November 2025 in Oakland, California, I declare under penalty of perjury that the foregoing is true.



Brian Hofer,
on behalf of Secure Justice and himself

EXHIBIT A

SETTLEMENT AGREEMENT AND GENERAL RELEASE

Secure Justice, Inc. and Brian Hofer v. City of Oakland
Case No. RG21111681
Superior Court of California, County of Alameda

This Document is subject to Public Disclosure

This settlement agreement and general release ("Agreement") is entered into between Petitioners SECURE JUSTICE, INC. and BRIAN HOFER ("Petitioners") and Respondent CITY OF OAKLAND ("Respondent") (collectively the "Parties").

RECITALS

This Agreement is made with reference to the following facts:

A. On September 2, 2021, Petitioners filed a Petition for Writ of Mandate and Prohibition in the Superior Court of California, County of Alameda, Case No. RG21111681, alleging claims for failure to comply with the Public Records Act, violations of the City of Oakland's Surveillance Ordinance (O.M.C. section 9.64, et seq.), violation of the Racial and Identity Profiling Act (A.B. 953), and for the Office of the City Attorney's refusal to advise the City of Oakland Privacy Advisory Commission.

B. The petition was subsequently amended several times, with the operative Third Amended Petition for Writ of Mandate or Prohibition filed on or about March 10, 2023. The Third Amended Petition alleges claims for failure to comply with the Public Records Act, violations of the City of Oakland's Surveillance Ordinance (O.M.C. section 9.64, et seq.), violation of the Racial and Identity Profiling Act (A.B. 953), and failure to perform mandatory duties under Civil Code section 1798.90.5 et seq. The facts, claims, and issues raised by the initial Petition through to the Third Amended Petition and any related facts, claims, or issues arising since the Third Amended Petition was filed through the Effective Date of this Agreement, are referred to as "the Dispute."

C. On October 24, 2023, the Parties participated in a mediation with Geri Green, Esq., and reached an agreement to settle the Dispute. That agreement was set forth in a Settlement Term Sheet attached hereto as Exhibit A. As reflected in the Settlement Term Sheet, the agreement was conditioned on approval of the settlement by the Oakland City Council, and the Oakland City Council has subsequently approved of the settlement on December 19, 2023. The Settlement Term Sheet further provided that the Parties would execute a full and complete release, which is this Agreement.

D. The Parties desire to settle and compromise the Dispute between the Parties on a mutually acceptable basis, and release any and all other claims, the specific terms and conditions of which settlement are embodied herein. This Agreement is not an admission of liability and Respondent expressly denies any liability.

NOW THEREFORE, in consideration of the covenants and promises herein set forth, the Parties hereto agree as follows:

TERMS

1. **Incorporation of recitals.** Paragraphs A through D of the Recitals are incorporated as though fully set forth herein.

2. **Settlement amount.** In consideration for the mutual covenants and promises herein contained and other good and valuable consideration, the receipt of which is hereby acknowledged, Respondent agrees to pay the sum of $30,000.00 (thirty-thousand dollars and zero cents) to Petitioners. Payment will be made within thirty (30) calendar days of the Effective Date of this Agreement. The check shall be made payable to "Secure Justice, Inc., Brian Hofer, and the Law Office of Mitchell Chyette."

3. **Dismissal of litigation.** Petitioners will dismiss with prejudice the subject litigation and will withdraw or dismiss any other complaint, claim, grievance, or charge that they have filed against Respondent pertaining in any way to the Dispute within seven (7) calendar days of receipt of the settlement payment from Respondent.

4. **Additional non-monetary terms.**

The Parties agree to the following non-monetary terms of settlement:

A. The Oakland Police Department (OPD) affirms that, in compliance with DGO I-12 (Automated License Plate Readers), as amended and approved by the City Council on October 17, 2023, all ALPR data older than 30 days, including all data within OPD's prior ALPR system, shall be destroyed. OPD will confirm this when it provides its update to the Public Safety Committee within 90 days of activation of the new ALPR system.

B. Any new ALPR technology used by OPD must comply with the then-applicable version of DGO I-12.

C. OPD affirms that it will comply with DGO I-20 (Gunshot Location Detection System ["GLDS"]) and particularly its provisions governing releasing or sharing GLDS data. OPD may seek revision of DGO I-20 to clarify the manner in which access to GLDS data is provided to the Oakland Housing Authority and prosecutorial agencies, in accordance with O.M.C. Ch. 9.64.

D. OPD will present to the City Council an ordinance codifying its use policy for its Forward Looking Infrared Thermal Imaging Camera System (FLIR) within 90 days of the Effective Date. OPD affirms that it is not using Domain Awareness Center or Cell Site Simulator technology. Should OPD commence use of the Domain Awareness Center or resume use of Cell Site Simulator technology, it will present to the City Council an ordinance codifying its use policy for those technologies within 90 days of such use.

E. OPD will present to the Privacy Advisory Commission draft use policies for the following existing technologies: (1) cell phone data extraction technology, (2) pole cameras, (3) remote audio telecommunications software (e.g. Penlink), (4) cameras on robots, and (5) hostage "throw" phones pursuant to OMC section 9.64.020, with the first draft use policy presented within 90 days of the Effective Date.

5. **Attorney fees and costs.** The $30,000.00 payment referred to in paragraph 2 above is payment in full for attorney's fees, costs, and any other expenses incurred by the Petitioners for filing and prosecuting the Petitions referred to in the Recitals, paragraphs A and B. Petitioners waive any right to the Court for any additional compensation for attorney's fees, costs, or expenses incurred in the prosecution of the Petitions, the finalization of the Settlement Agreement, or otherwise related to the Dispute.

6. **Release of all claims.** In consideration of the covenants undertaken herein, Petitioners shall be deemed to have fully, finally, and forever released Respondent, and all of its departments, officers, employees, attorneys, and agents, from any and all claims, charges, grievances, complaints, allegations, and causes of action for compensation, damages, injunctive relief, declaratory relief, writ relief, costs, attorneys' fees or any other form of relief of any nature whatsoever, whether the existence, nature or extent of the released claim is known or unknown, suspected or unsuspected, which Petitioners have or might have, or which Petitioners at any time heretofore had or might have had, claimed to have or may claim to have against Respondent, and all of its departments, officers, employees, attorneys, and agents, arising in, or in connection with, or out of the litigation described above and any such claim arising in, or in connection with, or out of the Dispute. The parties released as described in this paragraph are the "Released Parties" and the claims released as described in this paragraph are the "Released Claims."

7. **Waiver of California Civil Code Section 1542.** Petitioners recognize and acknowledge that factors which have induced them to enter into this Agreement may turn out to be incorrect or to be different from what they had previously anticipated, and Petitioners hereby expressly assume any and all of the risks thereof and further expressly assume the risks of waiving the rights provided by California Civil Code section 1542, which provides:

> "A general release does not extend to claims that the creditor or releasing party does not know or suspect to exist in his or her favor at the time of executing the release and that, if known by him or her, would have materially affected his or her settlement with the debtor or released party."

8. **No admissions.** This Agreement affects claims and demands which are disputed, and by executing this Agreement, no party admits or concedes any of the claims, defenses, or allegations which were raised or could be raised by any other party or any third party. Neither this Agreement nor any part of this Agreement shall be construed to be an admission by any party of any violation of law, nor shall this Agreement nor any part of it, nor any settlement negotiations or earlier drafts of this Agreement, be admissible in any proceeding as evidence of such an

admission. This document may be introduced in a proceeding solely to enforce the terms of this Agreement, and may be pleaded as a full and complete defense to any action, suit or other proceeding that has been or may be instituted, prosecuted or attempted with respect to any of the Released Claims.

9. **Warranty of non-assignment.** Petitioners warrant that they have not assigned any of the claims or portions of the claims that are the subject of this Agreement.

10. **No unwritten representations.** Each party represents that in executing this Agreement, the party does not rely upon and has not relied upon any representation, promise, or statement not expressly contained herein.

11. **Complete agreement.** This Settlement Agreement and General Release is the complete agreement between the Parties and supersedes any prior agreements or discussions between the parties.

12. **Tax consequences.** The Released Parties make no representation as to the tax consequences of the settlement or this Agreement.

13. **California law.** This Agreement is executed and delivered in the State of California, and the rights and obligations of the Parties hereunder shall be construed and enforced in accordance with the laws of the State of California.

14. **Interpretation and construction.** Any ambiguities or uncertainties herein shall be equally and fairly interpreted and construed without reference to the identity of the party or parties preparing this document or the documents referred to herein, on the understanding that the Parties participated equally in the negotiation and preparation of the Agreement and the documents referred to herein or have had equal opportunity to do so. This Agreement has been arrived at through negotiation and none of the Parties is to be deemed the party which prepared this Agreement or caused any uncertainty to exist within the meaning of Civil Code section 1654. The headings used herein are for reference only and shall not affect the construction of the Agreement. The Settlement Term Sheet may be considered in interpreting or construing this Agreement; provided, however, that in the event of a conflict between the two, this Agreement supersedes the Settlement Term Sheet.

15. **Breach, waiver and amendment.** No breach of this Agreement or of any provision herein can be waived except by an express written waiver executed by the party waiving such breach. Waiver of any one breach shall not be deemed a waiver of any other breach of the same or any other provision of this Agreement. This Agreement may be amended, altered, modified or otherwise changed in any respect or particular only by a writing duly executed by the Parties hereto or their authorized representatives.

16. **Authority to execute.** Each party hereto warrants to the other parties that it has the full power and authority to execute, deliver and perform under this Agreement and all documents

referred to herein, and that any needed consent or approval from any other person has been obtained.

17. **Counterparts.** This Agreement may be executed by the Parties in any number of counterparts, all of which taken together shall be construed as one document. Any facsimile or electronic signature shall be valid and acceptable for all purposes as if it were an original.

18. **Effective date.** The Effective Date of this Agreement shall be the date the last signatory hereto signs the Agreement.

19. **Duty to act in good faith.** The Parties shall act in good faith and use their reasonable good faith efforts after the execution of this Agreement to ensure that their respective obligations hereunder are fully and punctually performed. The Parties shall promptly perform any further acts and execute and deliver any other documents or instruments that may be reasonably necessary to carry out the provisions of this Agreement.

20. **Binding on successors and assigns.** This Agreement and all documents referred to herein shall bind and inure to the benefit of each of the Parties hereto, their administrators, representatives, executors, attorneys, successors, and assigns.

21. **No third-party beneficiaries.** Except as expressly provided herein, this Agreement is not for the benefit of any person not a party hereto or any person or entity not specifically identified as a beneficiary herein or specifically identified herein as a person or entity released hereby. The Agreement is not intended to constitute a third-party beneficiary contract.

22. **Agreement signed knowingly and voluntarily after opportunity to consult with counsel.** Petitioners understand and agree to this settlement agreement and to the terms and conditions contained herein and enter into this Agreement knowingly and voluntarily. The Parties have been advised that they have the right to seek legal advice with respect to this Agreement, including the release, and have consulted with their legal counsel regarding this Agreement. The Parties have investigated the facts pertaining to this Agreement and all matters pertaining thereto as deemed necessary. The Parties have relied on their judgment, belief, knowledge, understanding and expertise after consultation with their counsel concerning the legal effect of the settlement and its terms.

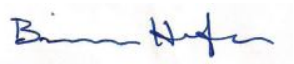
23. **Savings clause.** If any term, condition, provision, or part of this Agreement is determined to be invalid, void, or unenforceable for any reason, the remainder of this Agreement will continue in full force and effect.

IN WITNESS WHEREOF, the Parties hereto have executed this Settlement Agreement and Release:

Dated: _January 3, 2023__

Secure Justice, Inc.
By: BRIAN HOFER
Executive Director and Chairperson, Authorized Representative

Dated: __January 3, 2023_



BRIAN HOFER

Dated: __January 3, 2024_____

City of Oakland
By: KEVIN P. MCLAUGHLIN
Supervising Deputy City Attorney,
Authorized Representative

APPROVED AS TO FORM:

Dated: 1/3/2024_____

MITCHELL CHYETTE
Attorney for Petitioners

3322953

EXHIBIT A

Secure Justice & Brian Hofer v. City of Oakland
Case No. RG21111681

Settlement Term Sheet

Petitioners Secure Justice, Inc. and Brian Hofer filed a petition for writ of mandate and/or prohibition against Respondent City of Oakland in the above case.

The parties attended a mediation with Geri Green, Esq. on October 24, 2023. At the mediation the parties, through their authorized representatives, tentatively agreed as follows:

1. The Oakland Police Department (OPD) affirms that, in compliance with DGO I-12 (Automated License Plate Readers), as amended and approved by the City Council on October 17, 2023, all ALPR data older than 30 days, including all data within OPD's prior ALPR system, shall be destroyed. OPD will confirm this when it provides its update to the Public Safety Committee within 90 days of activation of the new ALPR system.
2. Any new ALPR technology used by OPD must comply with the then-applicable version of DGO I-12.
3. OPD affirms that it will comply with DGO I-20 (Gunshot Location Detection System) and particularly its provisions governing releasing or sharing GLD system data. OPD may seek revision of DGO I-20 to clarify the manner in which access to GLD system data is provided to the Oakland Housing Authority and prosecutorial agencies, in accordance with OMC Ch. 9.64.
4. OPD will present to the City Council an ordinance codifying its use policy for its Forward Looking Infrared Thermal Imaging Camera System (FLIR) within 90 days of the execution of a settlement agreement embodying the terms of this term sheet. OPD affirms that it is not using Domain Awareness Center or Cell Site Simulator technology. Should OPD resume using a Domain Awareness Center or Cell Site Simulator technology, it will present to the City Council an ordinance codifying its use policy for those technologies within 90 days of resuming use.
5. OPD will present to the Privacy Advisory Commission draft use policies for the following existing technologies: (1) cell phone data extraction technology, (2) pole cameras, (3) remote audio telecommunications software (e.g. Penlink), (4) cameras on robots, and (5) hostage "throw" phones pursuant to OMC section 9.64.020, with the first draft use policy presented within 90 days of the execution of a settlement agreement embodying the terms of this term sheet.
6. The City of Oakland will pay to Petitioners attorneys' fees and costs in the amount of $30,000.00. This amount includes all attorneys' fees and costs to date ~~and any fees or costs associated with enforcement of a settlement agreement embodying the terms of this term sheet.~~ KM BH
7. Petitioners will release and dismiss the City of Oakland and all of its departments, commissions, agents, officers, and employees from all claims alleged in the petition.
8. The parties' tentative agreement set forth in this term sheet is subject to approval by the Oakland City Council. Should the City Council not approve this tentative agreement, this term sheet is null and void. Should the City Council approve this tentative agreement, the parties will cooperate in good faith in reducing the terms of this term sheet to a written settlement agreement. That settlement agreement will include a Civil Code section 1542 release of

Petitioners' claims. Upon execution of that settlement agreement, Petitioners will file a request for dismissal with prejudice of their petition.

Date: 10/24/23

Brian Hofer, individually and for Secure Justice, Inc.

Date: 10/24/23

Kevin McLaughlin, for City of Oakland

EXHIBIT B

DEPARTMENTAL GENERAL ORDER

I-12: AUTOMATED LICENSE PLATE READERS

Effective Date: 14 AUG 24
Coordinator: Information Technology Unit

This policy provides guidance for the capture, storage and use of digital data obtained through the use of ALPR technology while recognizing the established privacy rights of the public.

A. Definitions

A - 1. Automated License Plate Reader (ALPR)

A device that uses cameras and computer technology to compare digital images of vehicle license plates to lists of known information of interest.

A - 2. Hot List

A list of license plates associated with vehicles of interest compiled from one or more databases including, but not limited to the Stolen Vehicle System (SVS), NCIC, and local BOLO alerts.

A - 3. Hit

Alert from the ALPR system that a scanned license plate may be in the National Crime Information Center (NCIC) or other law enforcement database for a specific reason including, but not limited to, being related to a stolen car, wanted person, missing person or domestic violence protective order.

B. Description of the Technology: *Information describing the surveillance technology and how it works.*

OPD uses Automated License Plate Reader (ALPR) technology to capture and store digital license plate data and images. There are two components to the ALPR system:

1. Automated License Plate Readers

Device components include cameras which can be attached to vehicles or fixed objects and a vehicle-based computer that processes the photographs and compares the data against California Department of Justice (CA DOJ) hot lists. Data are transmitted for comparison (the hot lists are downloaded to the vehicle at the start of the patrol shift and then compared from that list). Authorized/designated personnel can also manually enter license plates to internal OPD generated hot lists only accessible to personnel authorized/designated to access the OPD ALPR system.

2. ALPR Database

A central repository stores data collected and transmitted by the Automated License Plate Readers.

C. Purpose of the Technology

ALPR technology works by automatically and indiscriminately scanning all license plates on vehicles that are publicly visible. ALPR reads these license plates, compares the license plate characters against Hot Lists, and stores the characters along with the date, time, and location where the photograph was taken. This process allows for two functions by ALPR:

- Immediate (real time) comparison of the license plate characters against Hot Lists listing vehicles that are stolen or sought in connection with a crime and/or with OPD-generated internal lists.
- Storage of the license plate characters – along with the date, time, and location where the photography was taken – in a database that is accessible to enforcement agencies with authorized access (as defined in "Authorized Use" below) for investigative query purposes.

D. Authorized Uses

The specific uses that are authorized, and the rules and processes required prior to such use.

D - 1. Authorized Users

Personnel authorized/designated to use ALPR equipment or access information collected through the use of such equipment shall be specifically trained in such technology. Sworn personnel, Police Service Technicians (PST), or other authorized/designated Department personnel may use the technology. Authorized users other than sworn personnel or PSTs must be designated by the Chief of Police or designee.

D - 2. Authorized Use

- **Real-Time Identification**

The sworn personnel/technician shall verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before possibly taking enforcement action that is based solely on an ALPR alert.

Once an alert is received, the operator shall confirm that the observed license plate from the system matches the license plate of the observed vehicle.

Members will not take any police action that restricts the freedom of any individual based solely on an ALPR alert unless it has been fully validated, by visually verifying that the license plate characters on the vehicle match those in the database, and that the make, model, color and all other known identifying characteristics likewise match.

- **Hot Lists**

The Department shall only use the following hot lists: Stolen Vehicle System ("SVS"), National Crime Information Center ("NCIC") lists, CA DOJ lists, Amber and Silver alerts, and custom BOLO lists pertaining solely to missing or at-risk persons, witness locates, burglaries, grand

theft, and violent crime investigation. Hot lists shall be obtained or compiled from sources as may be consistent with the purposes of the ALPR system set forth in this Policy. Hot lists utilized by the Department's ALPR system may be updated by agency sources more frequently than the Department may be uploading them and thus the Department's ALPR system will not have access to real time data. Occasionally, there may be errors in the ALPR system's read of a license plate. Therefore, an alert alone shall not be a basis for police action (other than following the vehicle of interest). Prior to initiation of a stop of a vehicle or other intervention based on an alert, Department members shall undertake the following:

Department members will document all stops from hot list alerts by indicating the positive ALPR Hit, i.e., with an arrest or other enforcement action on a computer generated spreadsheet that **shall include** at minimum;

1. the Department member's name that responded to the alert,
2. the justification for responding to the alert,
3. the related case number,
4. the disposition code,
5. time and date of the response, and
6. any known next steps or follow up (e.g. forwarding case to District Attorney, alerting owner to recovered stolen vehicle).

- **Database Investigative Queries**

  Historical searches of scanned plates is permissible solely for missing or at-risk persons, witness locates, burglaries, grand theft, violent crime investigation, and in response to any subpoena, warrant, or other court order. Accessing the data shall be based on a standard of Reasonable Suspicion or greater. For each query, the Department **shall** record;

  1. the date and time the information is accessed,
  2. the license plate number or other data elements used to query the ALPR system,
  3. the username of the person who accesses the information, and, as applicable, the organization or entity with whom the person is affiliated, and
  4. the purpose for accessing the information. These records shall be attached to the annual report required by O.M.C. 9.64 et seq.

- **General Hot Lists** (such as SVS and NCIC) will be automatically downloaded into the ALPR system a minimum of once a day with the most current data overwriting the old data.

D - 3. All entries and updates of specific Hot Lists within the ALPR system will be documented by the requesting Department member within the appropriate

general offense report. All entries shall be approved by the ALPR Administrator (or his/her designee) before initial entry within the ALPR system. The hits from these data sources should be viewed as informational; created solely to bring the officers attention to specific vehicles of interest that might have been associated with criminal activity.

All Hot Plates and suspect information entered into the ALPR system will contain the following information as a minimum:

1. Entering Department member's name.
2. Related case number.
3. Justification for entering the plate and/or other identifying information onto the Hot List.
4. Date and time of entry.

E. Restrictions on Use

E - 1. Permitted/Impermissible Uses

All ALPR recordings collected from ALPR cameras installed on Oakland property are the property of the Oakland Police Department. Department personnel may only access and use the ALPR system consistent with this Policy. The following uses of the ALPR system are specifically prohibited:

- **Invasion of Privacy**: Except when done pursuant to a court order such as a search warrant, it is a violation of this Policy to utilize the ALPR to record license plates except those of vehicles that are exposed to public view (e.g., vehicles on a public road or street, or that are on private property but whose license plate(s) are visible from a public road, street, or a place to which members of the public have access, such as the parking lot of a shop or other business establishment). OPD shall make reasonable efforts to restrict the usage of the ALPR technology to the public right of way and other public property in alignment with this restriction.
- **Harassment or Intimidation**: It is a violation of this Policy to use the ALPR system to harass and/or intimidate any individual or group.
- **Use Based on a Protected Characteristic**: It is a violation of this policy to use the ALPR system or associated scan files or hot lists solely because of a person's, or group's race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law.
- **Personal Use**: It is a violation of this Policy to use the ALPR system or associated scan files or hot lists for any personal purpose.
- **First Amendment Rights**: It is a violation of this policy to use the ALPR system or associated scan files or hot lists for the purpose or known effect of infringing upon First Amendment rights.

- **Medical Rights**: No data from ALPR shall be used or shared with other agencies for the purpose of pursuing criminal charges or civil enforcement against individuals for obtaining, providing, or supporting reproductive health care services, to ensure that medical rights of residents of and visitors to Oakland, a Sanctuary City, remain intact.

  The Oakland Police Department or the City of Oakland shall solicit written documentation from the requesting agency confirming that the requested data from ALPR is not intended to be used for the prohibited purposes set forth herein. Such information shall be provided to all OPD sworn personnel responsible for providing the requested data.

  Department members shall not use, or allow others to use, the equipment or database records for any unauthorized purpose (Civil Code §798.90.51.; Civil Code § 1798.90.53).

  1. No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.
  2. No ALPR operator may access department, state or federal data unless otherwise authorized/designated to do so pursuant to Section E "Data Access" below.
  3. Accessing data collected by ALPR requires a right to know and a need to know. A right to know is the legal authority to receive information pursuant to a state or federal statute, applicable case law, or a court order. A need to know is a compelling reason to request information such as involvement in an active investigation.

F. Data Collection

The information that can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including "open source" data.

ALPR technology works by automatically scanning license plates on vehicles that are publicly visible. ALPR reads these license plates, compares the license plate characters (as well as vehicle attributes such as vehicle color or make and model with some ALPR systems) against specific databases, and stores the characters along with the date, time, and location where the photograph was taken, in a database.

G. Data Access

The category of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information.

Department sworn personnel, police service technicians, or other authorized/designated Department personnel may use the technology. Authorized/designated users other than sworn personnel or PSTs must be designated by the Chief of Police or designee.

Data may not be shared with out of state or federal agencies, per California law.

The Oakland Police Department does not permit the sharing of ALPR data gathered by the city or its contractors/subcontractors for purpose of federal immigration enforcement, pursuant to the California Values Act (Government Code § 7282.5; Government Code § 7284.2 et seq) – these federal immigration agencies include Immigration and Customs Enforcement (ICE) and Customs and Border Patrol (CPB).

All data and images gathered by the ALPR are for the official use of this department. Some information may not be disclosable to the general public. Investigatory records are not generally disclosable in response to a public records request. Non-investigatory records shall be disclosed in response to a public records request.

H. Data Protection

The safeguards that protect information from unauthorized access, including encryption and access control mechanisms.

All data shall be safeguarded and protected by both procedural and technological means. OPD shall observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

1. All ALPR server data shall be accessible only through a login/password-protected system capable of documenting all access of information by username, license number or other data elements used in the search, name, date, time and purpose. (Civil Code § 1798.90.52).
2. Data will be transferred from ALPRs to the designated storage per the ALPR technology data transfer protocol.

I. Data Retention

The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period.

All ALPR data uploaded to the server shall be purged from the server at the point of 30 days from initial upload. ALPR information may be retained outside this retention limit solely for the following purposes:

1. Active Criminal Investigations
2. Missing or at-risk Persons Investigations
3. Investigations from other law enforcement or prosecutorial agencies where there is a legal obligation to retain information.

J. Public Access: *how collected information can be accessed or used by members of the public, including criminal defendants.*

Requests for ALPR information by non-law enforcement or non-prosecutorial agencies will be processed in accordance with Civil Code § 1798.90.55, Government Code § 7920.000 et seq., this policy, and applicable case law and court orders.

K. Third Party Data Sharing: *If and how other City departments, bureaus, divisions, or non-City entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information.*

ALPR server data may be shared only as otherwise permitted by law and this policy. All data and images gathered by the ALPR are for the official use of this Department.

OPD has executed an MOU that grants CHP access to OPDs ALPR data for the duration of the MOU.

OPD personnel may share ALPR server data when there is a legal obligation to do so, such as a subpoena, court order or warrant to share such information, such as the following:

- a District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence;
- a Public Defender's Office or criminal defense attorney via the District Attorney's Office in accordance with applicable California criminal discovery laws;
- California law enforcement agencies as part of a formal criminal or administrative investigation;
- a party to civil litigation, or other third parties, in response to a valid court order only.

When there is no legal obligation to provide the requested data, requests for ALPR server data from other California law enforcement agencies shall be made in writing and may only be approved by the BOS Deputy Director/Chief or designee per the 3-step protocol below. These requests shall be maintained in a secure folder so that information about these requests can be shared in required annual reports with the PAC. Server access shall be restricted only to authorized/designated OPD personnel who will extract the required information and forward it to the requester.

1. The requesting party shall have a right to know, and a need to know. A right to know is the legal authority to receive information pursuant to a court order, statutory law, case law, or sworn officer status. A need to know is a compelling reason to request information such as direct involvement in an investigation.
2. The Department shall record the requesting party’s name and document the

right and need to know the requested information.

3. The Department shall record whether the request was honored or denied, the reason for such action, and the name of the Department officer that processed the request.

L. Training: *The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology.*

The Training Section shall ensure that members receive department-approved training for those authorized/designated to use or access the ALPR system and shall maintain a record of all completed trainings. (Civil Code § 1798.90.51; Civil Code §1798.90.53).

Training requirements for employees shall include the following:

- Applicable federal and state law
- Applicable policy
- Functionality of equipment
- Accessing data
- Safeguarding password information and data
- Sharing of data
- Reporting breaches
- Implementing post-breach procedures

M. Auditing and Oversight

The mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy.

Login/Log-Out Procedure. To ensure proper operation and facilitate oversight of the ALPR system, all users will be required to have individual credentials for access and use of the systems and/or data, which has the ability to be fully audited. It is the responsibility of the Department under this policy to actively pursue software and hardware upgrades that are needed to maintain full compliance with Section K of the use policy.

The records of Database Investigatory Queries, Third Party Data Sharing, and Hot List entries shall be incorporated into the annual report required by O.M.C. 9.64 et seq.

ALPR system audits shall be conducted annually to ensure proper system functionality and that designated personnel are using the system according to policy rules via sample audits, and reviews of training records. The size of these audits shall be large enough to provide a statistically significant representation of the

data collected.

N. Maintenance

The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.

N - 1. ALPR Administration

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the BOS. The BOS may contract with an ALPR service provider for installation and maintenance assistance.

N - 2. ALPR Administrator

The BOS Deputy Director/Chief shall be the administrator of the ALPR program, and shall be responsible for developing guidelines and procedures to comply with the requirements of Civil Code § 1798.90.5 et seq. The BOS Deputy Director/Chief is responsible for ensuring systems and processes are in place for the proper collection, and retention of ALPR data.

N - 3. ALPR Coordinator:

The title of the official custodian of the ALPR system is the ALPR Coordinator.

N - 4. Monitoring and Reporting

The Oakland Police Department will ensure that the system is remains functional according to its intended use and monitor its use of ALPR technology to ensure the proper functionality of the system as defined in the policy guidelines of this document, including required audits, training, and data access records.

N - 5. The ALPR Coordinator shall provide the Chief of Police, Privacy Advisory Commission, and Public Safety Committee with an annual report pursuant to OMC 9.64 (Oakland Surveillance Technology Ordinance).

By Order of,

Floyd Mitchell
Chief of Police

Date: 8-14-24

EXHIBIT C

Chapter 9.64 REGULATIONS ON CITY'S ACQUISITION AND USE OF SURVEILLANCE TECHNOLOGY

9.64.010 Definitions.

The following definitions apply to this Chapter.

1. "Annual Surveillance Report" means a written report concerning a specific surveillance technology that includes all the following:

    A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology;

    B. Whether and how often data acquired through the use of the surveillance technology was directly shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);

    C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to;

    D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year;

    E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties.

The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review;

    F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information.

    G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response;

    H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes;

    I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates;

J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year; and

K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request.

2. "Biometric Surveillance Technology" means any computer software that uses face recognition technology or other remote biometric recognition in real time or on a recording or photograph.

3. "City" means any department, agency, bureau, and/or subordinate division of the City of Oakland as provided by Chapter 2.29 of the Oakland Municipal Code.

4. "City Staff" means City personnel authorized by the City Administrator or designee to seek City Council approval of surveillance technology in conformance with this Chapter.

5. "Continuing Agreement" means an agreement that automatically renews unless terminated by one (1) party.

6. "Exigent Circumstances" means a law enforcement agency's good faith belief that an emergency involving danger of, or imminent threat of the destruction of evidence regarding, death or serious physical injury to any person requires the use of surveillance technology or the information it provides.

7. "Face Recognition Technology" means an automated or semi-automated process that: (A) assists in identifying or verifying an individual based on an individual's face; or (B) identifies or logs characteristics of an individual's face, head, or body to infer emotion, associations, expressions, or the location of an individual.

8. "Large-Scale Event" means an event attracting ten thousand (10,000) or more people with the potential to attract national media attention that provides a reasonable basis to anticipate that exigent circumstances may occur.

9. "Other Remote Biometric Recognition" means: (A) an automated or semi-automated process that (i) assists in identifying an individual, capturing information about an individual, or otherwise generating or assisting in generating information about an individual based on physiological, biological, or behavioral characteristics ascertained from a distance; (ii) uses voice recognition technology; or (iii) identifies or logs such characteristics to infer emotion, associations, activities, or the location of an individual; and (B) does not include identification based on fingerprints or palm prints that have been manually obtained during the course of a criminal investigation or detention.

10. "Personal Communication Device" means a mobile telephone, a personal digital assistant, a wireless capable tablet and a similar wireless two-way communications and/or portable internet accessing devices, whether procured or subsidized by a city entity or personally owned, that is used in the regular course of city business.

11. "Predictive Policing Technology" means computer algorithms that use preexisting data to forecast or predict places or times that have a high risk of crime, or individuals or groups who are likely to be connected to a crime. This definition does not include computer algorithms used solely to visualize, chart, or map past criminal activity (e.g. heat maps).

12. "Police Area" refers to each of the geographic districts assigned to a police commander and as such districts are amended from time to time.

13. "Surveillance" or "Surveil" means to observe or analyze the movements, behavior, data, or actions of individuals. Individuals include those whose identity can be revealed by license plate data when combined with any other record.

14. "Surveillance Technology" means any software, electronic device, system utilizing an electronic device, or similar technological tool used, designed, or primarily intended to collect, retain, analyze, process, or share audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically

associated with, or capable of being associated with, any individual or group. Examples of surveillance technology include, but is not limited to the following: cell site simulators (Stingrays); automatic license plate readers; gunshot detectors (ShotSpotter); facial recognition software; thermal imaging systems; body-worn cameras; social media analytics software; gait analysis software; video cameras that record audio or video, and transmit or can be remotely accessed. It also includes software designed to monitor social media services or forecast criminal activity or criminality, biometric identification hardware or software.

"Surveillance technology" does not include the following devices or hardware, unless they have been equipped with, or are modified to become or include, a surveillance technology as defined above:

A. Routine office hardware, such as televisions, computers, credit card machines, badge readers, copy machines, and printers, that is in widespread use and will not be used for any surveillance or law enforcement functions;

B. Parking Ticket Devices (PTDs);

C. Manually-operated, non-wearable, handheld digital cameras, audio recorders, and video recorders that are not designed to be used surreptitiously and whose functionality is limited to manually capturing and manually downloading video and/or audio recordings;

D. Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles;

E. Manually-operated technological devices used primarily for internal municipal entity communications and are not designed to surreptitiously collect surveillance data, such as radios and email systems;

F. City databases that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology, including payroll, accounting, or other fiscal databases.

G. Medical equipment used to diagnose, treat, or prevent disease or injury.

H. Police department interview room cameras.

I. Police department case management and records management systems, including computer aided dispatch systems, and field-based reporting systems.

J. Police department early warning systems.

K. Personal communication devices that have not been modified beyond stock manufacturer capabilities in a manner described above, provided that any bundled face recognition technology is only used for the sole purpose of user authentication in the regular course of conducting City business.

L. Live scan machines (owned by Alameda County Sheriff but operated by Oakland Police personnel.)

15. "Surveillance Impact Report" means a publicly-released written report including at a minimum the following:

A. Description: information describing the surveillance technology and how it works, including product descriptions and manuals from manufacturers;

B. Purpose: information on the proposed purposes(s) for the surveillance technology;

C. Location: the location(s) it may be deployed, using general descriptive terms, and crime statistics for any location(s);

D. Impact: an assessment of the technology's adopted use policy and whether it is adequate in protecting civil rights and liberties and whether the surveillance technology was used or deployed, intentionally or inadvertently, in a manner that is discriminatory, viewpoint-based, or biased via algorithm;

E. Mitigations: identify specific, affirmative technical and procedural measures that will be implemented to safeguard the public from each such impacts;

F. Data Types and Sources: a list of all types and sources of data to be collected, analyzed, or processed by the surveillance technology, including "open source" data, scores, reports, logic or algorithm used, and any additional information derived therefrom;

G. Data Security: information about the steps that will be taken to ensure that adequate security measures are used to safeguard the data collected or generated by the technology from unauthorized access or disclosure;

H. Fiscal Cost: the fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, operative or proposed contract, and any current or potential sources of funding;

I. Third Party Dependence: whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis;

J. Alternatives: a summary of all alternative methods (whether involving the use of a new technology or not) considered before deciding to use the proposed surveillance technology, including the costs and benefits associated with each alternative and an explanation of the reasons why each alternative is inadequate; and,

K. Track Record: a summary of the experience (if any) other entities, especially government entities, have had with the proposed technology, including, if available, quantitative information about the effectiveness of the proposed technology in achieving its stated purpose in other jurisdictions, and any known adverse information about the technology (such as unanticipated costs, failures, or civil rights and civil liberties abuses).

16. "Surveillance Use Policy" means a publicly-released and legally enforceable policy for use of the surveillance technology that at a minimum specifies the following:

A. Purpose: the specific purpose(s) that the surveillance technology is intended to advance;

B. Authorized Use: the specific uses that are authorized, and the rules and processes required prior to such use;

C. Data Collection: the information that can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including "open source" data;

D. Data Access: the category of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information;

E. Data Protection: the safeguards that protect information from unauthorized access, including encryption and access control mechanisms;

F. Data Retention: the time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period;

G. Public Access: how collected information can be accessed or used by members of the public, including criminal defendants;

H. Third Party Data Sharing: if and how other city departments, bureaus, divisions, or non-city entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information;

I. Training: the training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology, and the category of staff that will provide the training;

J. Auditing and Oversight: the mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy; and

K. Maintenance: The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.

17. "Voice Recognition Technology" means the automated or semi-automated process that assists in identifying or verifying an individual based on the characteristics of an individual's voice.

(Ord. No. 13635, § 2, 1-12-2021; Ord. No. 13563, § 3, 9-17-2019; Ord. No. 13489, § 2, 5-15-2018)

9.64.020 Privacy Advisory Commission (PAC) notification and review requirements.

1. PAC Notification Required Prior to City Solicitation of Funds and Proposals for Surveillance Technology.

   A. City staff shall notify the Chair of the Privacy Advisory Commission prior to:

      1. Seeking or soliciting funds for new surveillance technology or to replace existing surveillance technology that has not been previously approved by the City Council pursuant to the requirements of this Chapter, including but not limited to applying for a grant; or,

      2. Soliciting proposals with a non-city entity to acquire, share or otherwise use surveillance technology or the information it provides.

   B. Upon notification by city staff, the Chair of the Privacy Advisory Commission shall place the item on the agenda at the next Privacy Advisory Commission meeting for discussion and possible action. At this meeting, city staff shall inform the Privacy Advisory Commission of the need for the funds or equipment, or shall otherwise justify the action city staff will seek Council approval for pursuant to 9.64.030. The Privacy Advisory Commission may make a recommendation to the City Council by voting its approval to proceed, object to the proposal, recommend that the city staff modify the proposal, or take no action.

   C. Should the Privacy Advisory Commission not make a recommendation pursuant to 9.64.020 1.B., City staff may proceed and seek Council approval of the proposed surveillance technology initiative pursuant to the requirements of Section 9.64.030.

2. PAC Review Required for New Surveillance Technology Before City Council Approval.

   A. Prior to seeking City Council approval under Section 9.64.030, city staff shall submit a surveillance impact report and a surveillance use policy for the proposed new surveillance technology initiative to the Privacy Advisory Commission for its review at a regularly noticed meeting. The surveillance impact report and surveillance use policy must address the specific subject matter specified for such reports as defined under 9.64.010.

   B. The Privacy Advisory Commission shall recommend that the City Council adopt, modify, or reject the proposed surveillance use policy. If the Privacy Advisory Commission proposes that the Surveillance

Use Policy be modified, the Privacy Advisory Commission shall propose such modifications to city staff. City staff shall present such modifications to City Council when seeking City Council approval under Section 9.64.030.

C. Failure by the Privacy Advisory Commission to make its recommendation on the item within ninety (90) days of submission shall enable the city entity to proceed to the City Council for approval of the item.

3. PAC Review Requirements for Existing Surveillance Technology Before City Council Approval.

A. Prior to seeking City Council approval for existing city surveillance technology under Section 9.64.030 city staff shall submit a surveillance impact report and surveillance use policy to the Privacy Advisory Commission for its review at a regularly noticed meeting. The surveillance impact report and surveillance use policy must address the specific subject matter specified for such reports as defined under 9.64.010.

B. Prior to submitting the surveillance impact report and proposed surveillance use policy as described above, city staff shall present to the Privacy Advisory Commission a list of surveillance technology possessed and/or used by the city.

C. The Privacy Advisory Commission shall rank the items in order of potential impact to civil liberties.

D. Within sixty (60) days of the Privacy Advisory Commission's action in 9.64.020 3.C., city staff shall submit at least one (1) surveillance impact report and proposed surveillance use policy per month to the Privacy Advisory Commission for review, beginning with the highest-ranking items as determined by the Privacy Advisory Commission, and continuing thereafter each month until a policy has been submitted for each item on the list.

City staff, acting on behalf of a particular department, agency, bureau, or other subordinate division of the City, is not required to submit a new surveillance impact report and surveillance use policy, until the Privacy Advisory Commission has completed its recommendation and analysis on any outstanding surveillance technology that has been previously submitted from such department, agency, bureau, or other subordinate division of the City.

E. Failure by the Privacy Advisory Commission to make its recommendation on any item within ninety (90) days of submission shall enable city staff to proceed to the City Council for approval of the item pursuant to Section 9.64.030.

(Ord. No. 13635, § 2, 1-12-2021; Ord. No. 13489, § 2, 5-15-2018)

9.64.030. City Council approval requirements for new and existing surveillance technology.

1. City staff must obtain City Council approval prior to any of the following:

A. Accepting state or federal funds or in-kind or other donations for surveillance technology, except for surveillance technology that has already been approved by City Council and for which a corresponding use policy is in effect;

B. Acquiring new surveillance technology, or replacing existing surveillance technology that has not been previously approved by the City Council pursuant to the requirements of this Chapter, including but not limited to procuring such technology without the exchange of monies or consideration;

C. Using new surveillance technology, or using existing surveillance technology or the information it provides for a purpose, in a manner, or in a location not previously approved by the City Council pursuant to the requirements of this Chapter. However, for surveillance technology that was acquired or was in use prior to enactment of this ordinance, such use may continue until the City Council votes to approve or reject the surveillance technology's corresponding surveillance use policy; or

D. Entering into a continuing agreement or written agreement with a non-city entity to acquire, share or otherwise use surveillance technology or the information it provides, including data sharing agreements.

E. Notwithstanding any other provision of this Section, nothing herein shall be construed to prevent, restrict or interfere with any person providing evidence or information derived from surveillance technology to a law enforcement agency for the purposes of conducting a criminal investigation or the law enforcement agency from receiving such evidence or information.

2. City Council Approval Process.

A. After the PAC notification and review requirements in Section 9.64.020 have been met, city staff seeking City Council approval shall schedule for City Council consideration and approval of the proposed surveillance impact report and proposed surveillance use policy, and include Privacy Advisory Commission recommendations. City Council consideration and approval may only occur at a public meeting that has been noticed in conformance with the Oakland Sunshine Ordinance. City staff shall not unreasonably delay scheduling any item for City Council consideration and approval at the next earliest opportunity.

B. The City Council shall only approve any action as provided in this Article after first considering the recommendation of the Privacy Advisory Commission, and subsequently making a determination that the benefits to the community of the surveillance technology outweigh the costs; that the proposal will safeguard civil liberties and civil rights; and that, in the City Council's judgment, no alternative with a lesser economic cost or impact on civil rights or civil liberties would be as effective.

C. For approval of existing surveillance technology for which the Privacy Advisory Commission failed to make its recommendation within ninety (90) days of review as provided for under 9.64.020 3.E, if the City Council has not reviewed and approved such item within four (4) City Council meetings from when the item was initially scheduled for City Council consideration, the city shall cease its use of the surveillance technology until such review and approval occurs.

3. Surveillance Impact Reports and Surveillance Use Policies are Public Records. City staff shall make the Surveillance Impact Report and Surveillance Use Policy, as updated from time to time, available to the public as long as the city uses the surveillance technology in accordance with its request pursuant to Section 9.64.020 A.1.

(Ord. No. 13635, § 2, 1-12-2021; Ord. No. 13489, § 2, 5-15-2018)

9.64.035 Use of unapproved technology during exigent circumstances or large-scale event.

1. City staff may temporarily acquire or use surveillance technology and the data derived from that use in a manner not expressly allowed by a surveillance use policy in two (2) types of circumstances without following the provisions of Section 9.64.030: (A) exigent circumstances, and (B) a large-scale event.

2. If city staff acquires or uses a surveillance technology in the two (2) circumstances pursuant to subdivision 1., the city staff shall:

A. Use the surveillance technology to solely respond to the exigent circumstances or large-scale event.

B. Cease using the surveillance technology when the exigent circumstances or large scale event ends.

C. Only keep and maintain data related to the exigent circumstances and dispose of any data that is not relevant to an ongoing investigation.

D. Following the end of the exigent circumstances or large-scale event, report that acquisition or use to the PAC at their next respective meetings for discussion and/or possible recommendation to the City Council in accordance with the Sunshine Ordinance, the Brown Act, and City Administrator deadlines.

3. Any technology temporarily acquired in exigent circumstances or during a large-scale event shall be returned within seven (7) days following its acquisition, or when the exigent circumstances end, whichever is sooner, unless the technology is submitted to the City Council for approval pursuant to Section 9.64.030 and is approved. If the agency is unable to comply with the seven-day timeline, the agency shall notify the City Council, who may grant an extension.

(Ord. No. 13489, § 2, 5-15-2018)

9.64.040 Oversight following City Council approval.

1. By April 30th of each year, or no later than one (1) year after adoption of a Surveillance Use Policy, city staff must present a written annual surveillance report for Privacy Advisory Commission review for each approved surveillance technology item. If city staff is unable to meet the deadline, city staff shall notify the Privacy Advisory Commission in writing of staff's request to extend this period, and the reasons for that request. The Privacy Advisory Commission may grant a single extension of up to sixty (60) days to comply with this provision.

   A. After review by the Privacy Advisory Commission, city staff shall submit the annual surveillance report to the City Council.

   B. The Privacy Advisory Commission shall recommend to the City Council that the benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded; that use of the surveillance technology cease; or propose modifications to the corresponding surveillance use policy that will resolve the concerns.

   C. Failure by the Privacy Advisory Commission to make its recommendation on the item within ninety (90) days of submission shall enable the city entity to proceed to the City Council for approval of the annual surveillance report.

   D. In addition to the above submission of any Annual Surveillance Report, city staff shall provide in its report to the City Council a summary of all requests for City Council approval pursuant to Section 9.64.030 and the pertinent Privacy Advisory Commission recommendation, including whether the City Council approved or rejected the proposal and/or required changes to a proposed surveillance use policy before approval.

2. Based upon information provided in city staff's Annual Surveillance Report and after considering the recommendation of the Privacy Advisory Commission, the City Council shall re-visit its "cost benefit" analysis as provided in Section 9.64.030 2.B. and either uphold or set aside the previous determination. Should the City Council set aside its previous determination, the city's use of the surveillance technology must cease. Alternatively, City Council may require modifications to the Surveillance Use Policy that will resolve any deficiencies.

(Ord. No. 13635, § 2, 1-12-2021; Ord. No. 13489, § 2, 5-15-2018)

9.64.045 Prohibition on City's acquisition and/or use of Biometric Surveillance Technology and Predictive Policing Technology.

A. Notwithstanding any other provision of this Chapter (9.64), it shall be unlawful for the City or any City staff to obtain, retain, request, access, or use:

1. Biometric Surveillance Technology; or
2. Predictive Policing Technology; or
3. Information obtained from either Biometric Surveillance Technology or Predictive Policing Technology.

B. Only surveillance technology that uses biometric information in a manner that meets the definition of Biometric Surveillance Technology, as provided in Section 9.64.010, shall be prohibited.

C. City staff's inadvertent or unintentional receipt, access of, or use of any information obtained from Biometric Surveillance Technology or Predictive Policing Technology shall not be a violation of this Section 9.64.045 provided that:

1. City staff did not request or solicit the receipt, access of, or use of such information; and
2. City staff shall immediately destroy all copies of the information upon its discovery and shall not use the information for any purpose, unless retention or use of exculpatory evidence is required by law; and
3. Upon discovery of such use, City staff logs such receipt, access, or use in a written report and submits such report at the next regularly scheduled meeting of the Privacy Advisory Commission for discussion and possible recommendation to the City Council. Such a report shall not include any personally identifiable information or other information the release of which is prohibited by law. In its report, City staff shall identify specific measures taken by the City to prevent the further transmission or use of any information inadvertently or unintentionally obtained through the use of such technologies; and
4. After review by the Privacy Advisory Commission, city staff shall submit the report to the City Council.

(Ord. No. 13635, § 2, 1-12-2021; Ord. No. 13563, § 3, 9-17-2019)

9.64.050 Enforcement.

1. Violations of this Article are subject to the following remedies:

A. Any violation of this Article, or of a surveillance use policy promulgated under this Article, constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in the Superior Court of the State of California to enforce this Article. An action instituted under this paragraph shall be brought against the respective city department, and the City of Oakland, and, if necessary to effectuate compliance with this Article or a surveillance use policy (including to expunge information unlawfully collected, retained, or shared thereunder), any other governmental agency with possession, custody, or control of data subject to this Article, to the extent permitted by law.

B. Any person who has been subjected to a surveillance technology in violation of this Article, or about whom information has been obtained, retained, accessed, shared, or used in violation of this Article or of a surveillance use policy promulgated under this Article, may institute proceedings in the Superior Court of the State of California against the City of Oakland and shall be entitled to recover actual damages (but not less than liquidated damages of one thousand dollars ($1,000.00) or one hundred dollars ($100.00) per day for each day of violation, whichever is greater).

C. A court shall award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in an action brought under paragraphs A. or B.

D. Violations of this Article by a city employee shall result in consequences that may include retraining, suspension, or termination, subject to due process requirements and in accordance with any memorandums of understanding with employee bargaining units.

(Ord. No. 13489, § 2, 5-15-2018)

9.64.060 Secrecy of surveillance technology.

It shall be unlawful for the city to enter into any surveillance-related contract or other agreement that conflicts with the provisions of this Article, and any conflicting provisions in such future contracts or agreements, including but not limited to non-disclosure agreements, shall be deemed void and legally unenforceable.

To the extent permitted by law, the city shall publicly disclose all of its surveillance-related contracts, including any and all related non-disclosure agreements, if any, regardless of any contract terms to the contrary.

(Ord. No. 13489, § 2, 5-15-2018)

9.64.070 Whistleblower protections.

1. Neither the city nor anyone acting on behalf of the city may take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee or applicant for employment, including but not limited to discriminating with respect to compensation, terms and conditions of employment, access to information, restrictions on due process rights, or civil or criminal liability, because:
    A. The employee or applicant was perceived to, about to, or assisted in any lawful disclosure of information concerning the funding, acquisition, or use of a surveillance technology or surveillance data based upon a good faith belief that the disclosure evidenced a violation of this Article; or
    B. The employee or applicant was perceived to, about to, or assisted or participated in any proceeding or action to carry out the purposes of this Article.
2. It shall be grounds for disciplinary action for a city employee or anyone else acting on behalf of the city to retaliate against another city employee or applicant who makes a good-faith complaint that there has been a failure to comply with any surveillance use policy or administrative instruction promulgated under this Article.
3. Any employee or applicant who is injured by a violation of this Section may institute a proceeding for monetary damages and injunctive relief against the city in any court of competent jurisdiction.

(Ord. No. 13489, § 2, 5-15-2018)

EXHIBIT D

DEPARTMENTAL GENERAL ORDER

I-24: FORENSIC LOGIC COPLINK

Effective Date:

Coordinator: Information Technology Unit

FORENSIC LOGIC COPLINK

The purpose of this order is to establish Departmental policy and procedures for the use of the Forensic Logic, LLC. CopLink Data System

VALUE STATEMENT

The purpose of this policy is to establish guidelines for the use of the Forensic Logic, LLC. CopLink law enforcement data search system. The Oakland Police Department (OPD) uses crime databases to provide OPD personnel with timely and useful information to investigate crimes and analyze crime patterns.

A. Purpose: *The specific purpose(s) that the surveillance technology is intended to advance*

Forensic Logic, Inc. ("Forensic Logic") built a data warehouse that integrates and organizes data from databases such as Computer Assisted Dispatch (CAD) and Records Management System (RMS) and other law enforcement information systems from different law enforcement agencies. Forensic Logic provides two core services for OPD: 1) crime analysis reports; and 2) data search.

1. Crime Analysis Report Production – Forensic Logic categorizes and organizes incidents by offense types that allows OPD crime analysts to produce crime analysis reports such as point in time year-to-date and year-to-year comparisons. The categorization takes thousands of penal code types and organizes the data in a comprehensive manner to tabulate data into standard Federal Bureau of Investigation (FBI) Uniform Crime Report Part One and Part Two crimes.
2. Search – OPD data (e.g., CAD/RMS) is searchable with other agency law enforcement data. Personnel can use the system to search crime reports for structured data (e.g., suspect names) and unstructured data (e.g., a vehicle description). The cloud-based search system is accessible via a secure internet web browser requiring user authentication from vehicle mobile data terminal (MDT), web-enabled computers on the OPD computer network, or via OPD-issued and managed mobile devices.

B. Authorized Use*: The specific uses that are authorized, and the rules and processes required prior to such use*

The authorized uses of Forensic Logic system access are as follows:

- Crime Analysis Report Production – Authorized members may use the customized system to organize OPD crime data into Crime Analysis Reports. Forensic Logic built a system that categorizes thousands of penal codes based on hierarchical crime reporting standards, into a concise, consumable report template.
- CopLink Search – Authorized members may use CopLink for the purpose of searching the system in the service of conducting criminal investigations, such as apprehending subjects, locating and returning stolen property, as well as in the protection of the law enforcement officers encountering the individuals described in the system. Authorized purposes also include other appropriate OPD organizational investigations (e.g., internal affairs, missing persons, and use of force investigations).

Rules and Processes Prior to use

- Only sworn law enforcement personnel or authorized professional staff employed and working under the supervision of a law enforcement agency (typically crime analysts and dispatchers) may access the Forensic Logic CopLink network.
- OPD personnel authorized to use Forensic Logic CopLink receive required security awareness training prior to using the system. Forensic Logic requires users to have the same training to access the Forensic Logic CopLink network as users are required to be trained to access data in CLETS, the FBI NCIC system or NLETS. Users are selected and authorized by OPD and OPD warrants that all users understand and have been trained in the protection of Criminal Justice Information (CJI) data in compliance with FBI Security Policy. All Forensic Logic CopLink users throughout the Forensic Logic CopLink network have received required training and their respective law enforcement agencies have warranted that their users comply with FBI CJI data access requirements.
- Users shall not use or allow others to use the equipment or database records for any unauthorized purpose; authorized purposes consist only of queries related to investigations, internal audits, or for crime analysts to produce crime analysis reports. The purpose of the Forensic Logic CopLink network is to provide a computerized database for ready access by a criminal justice agency making an inquiry and for prompt disclosure of information in the system from other criminal justice agencies about crimes and criminals. Users are required to abide by the Terms of Service of the Forensic Logic CopLink network when they access the system. The Terms of Service that every User agrees to include the following statements:
    1. *I will use the Forensic Logic Coplink Network™ only for the administration of criminal justice or the administration of data required to be stored in a secure sensitive but unclassified data environment.*

2. *I will respect the confidentiality and privacy of individuals whose records I may access.*
3. *I will observe any ethical restrictions that apply to data to which I have access, and to abide by applicable laws or policies with respect to access, use, or disclosure of information.*
4. *I agree not to use the resources of the Forensic Logic Coplink Network™ in such a way that the work of other users, the integrity of the system, or any stored data may be jeopardized.*

I am forbidden to access or use any Forensic Logic Coplink Network™ data for my own personal gain, profit, or the personal gain or profit of others, or to satisfy my personal curiosity.

- The following warning is displayed for every user session prior to user sign on:

  WARNING: *You are accessing sensitive information including criminal records and related data governed by the FBI's Criminal Justice Information System (CJIS) Security Policy. Use of this network provides us with your consent to monitor, record, and audit all network activity. Any misuse of this network and its data is subject to administrative and/or criminal charges. CJIS Security Policy does not allow the sharing of access or passwords to the Forensic Logic Coplink Network™. The data content of the Forensic Logic Coplink Network™ will not be considered for use as definitive probable cause for purposes of arrests, searches, seizures or any activity that would directly result in providing sworn testimony in any court by any participating agency. Information available in the Forensic Logic Coplink Network™ is not probable cause, but indicates that data, a report or other information exists in the Records Management System or other law enforcement, judicial or other information system of an identified participating agency or business.*

  In accordance with California Senate Bill 54, applicable federal, state or local law enforcement agencies shall not use any non-criminal history information contained within this database for immigration enforcement purposes. This restriction does not pertain to any information that is regarding a person's immigration or citizenship status pursuant to 8 U.S.C. §§ 1373 and 1644.

- Accessing CopLink data requires a right to know and a need to know. A right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law. A need to know is a compelling reason to request information such as direct involvement in a criminal investigation.

C. ***Data Collection:*** *The information that can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including "open source" data;*

Forensic Logic has created a file transfer protocol to automatically ingest several data systems into the Forensic Logic CopLink system. These databases include

CAD/RMS and FBR. Additionally, OPD is discussing the possibility of incorporating National Integrated Ballistic Information Network (NIBIN) firearm shell casing data into the system. No ALPR data collected by OPD-owned technology shall be extracted by Forensic Logic's systems. An exhaustive list of data sets ingested by Forensic Logic CopLink from OPD data sources follows.

Data Source Collected	Collection Status	Retention Policy	Access Conditions
Arrest	Active	Perpetual	Only law enforcement; US DHS prohibited
Field Contacts	Active	Perpetual	Only law enforcement; US DHS prohibited
Incident Reports	Active	Perpetual	Only law enforcement; US DHS prohibited
Calls for Service	Active	Perpetual	Only law enforcement; US DHS prohibited
Stop Data	Active	Perpetual	Only law enforcement; US DHS prohibited
Traffic Accident	Active	Perpetual	Only law enforcement; US DHS prohibited
ShotSpotter	Active	Perpetual	Only law enforcement; US DHS prohibited
ATF NIBIN Ballistics	Proposed	Perpetual	Only law enforcement; US DHS prohibited

There are several "Elements of the Search" component – all of which are specialized presentations of search[1]: (see related Surveillance Impact Report for a detailed analysis:

- The search bar;
- The Tag Cloud element - how search results are visualized by increasing the font size in a Tag Cloud to be representative of the number of occurrences;
- Facet search - organizes search capabilities into a number of static

[1] See related Surveillance Impact Report for a detailed description of each 'search' module

categories (e.g. offense descriptions, agencies);

- Time Search - permits users to quickly drill down to specific time periods;
- Timeline search - organizes the data visually on a timeline;
- Geospatial search - permits a user to select geographies (e.g. Beats or Areas; areas around schools, custom areas);
- Search Charting Module - organizes search results into categories visualized by bar charts;
- Link Chart - produces a visualization of records that are linked based on several criteria including name, offense and location.

Forensic Logic CopLink also consists of the following modules:

- CopLink Connect (formerly called forums);
- CopLink Dashboard, and CopLink Trace (gun-tracing);
- CopLink Connect - a secure internal communication system for intra-agency CJIS-compliant communications.

D. Data Access: *The category of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information*

Authorized users include all sworn personnel, Crime Analysts, Police Evidence Technicians, personnel assigned to OIG, and other personnel as approved by the Chief of Police.

OPD data in the Forensic Logic CopLink system is owned by OPD and not Forensic Logic and is drawn from OPD underlying systems. OPD personnel shall follow all access policies that govern the use of those originating OPD technologies.

OPD's Information Technology (IT) Unit shall be responsible ensuring ongoing compatibility of the Forensic Logic CopLink System with OPD computers and MDT computer systems. OPD's IT Unit will assign personnel to be responsible for ensuring system access and coordinate with Forensic Logic. CopLink Search users are managed through a centralized account management process by Forensic Logic support personnel.

E. Data Protection: *The safeguards that protect information from unauthorized access, including encryption and access control mechanisms;*

Forensic Logic constantly processes large streams of criminal justice information (CJI) and thus must comply with the provisions of the Criminal Justice Information Services (CJIS) Division of the Federal Bureau of Investigation (FBI) and the FBI

Security Management Act of 2003 and CJIS Security Policy. Forensic Logic, along with their partner at Microsoft Azure Government and the National Law Enforcement Telecommunications System (NLETS), have developed strong CJIS-compliant data security protocols.

F. Data Retention*: The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period;*

Forensic Logic follows the data retention schedules reflective of OPD's data retention schedules. Data that is deleted from OPD CAD/RMS or other systems will be automatically deleted from Forensic Logic CopLink system. OPD can also request that OPD data be expunged from the Forensic Logic CopLink system where appropriate based on changes to incident files.

G. Public Access*: How collected information can be accessed or used by members of the public, including criminal defendants;*

The Weekly Crime Analysis Reports prepared using Forensic Logic's analysis of OPD crime data are regularly made available to the public on OPD's website. The CopLink system is only provided for OPD personnel and is not available to the public.

H. Third Party Data Sharing: *If and how other City departments, bureaus, divisions, or non-City entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information;*

Other than selected individuals with a right to access at ITD, no other non-OPD City entities may access the Forensic Logic system. Many law enforcement agencies (city police departments and county sheriff offices) utilize Forensic Logic CopLink. ***Attachment A*** to this Use Policy provides a list of agencies[2] that are clients of Forensic Logic and have access to OPD data through CopLink Search.

Many law enforcement agencies that are clients of Forensic Logic have access to OPD data through CopLink – a complete list is provided in ***Appendix D*** to the CopLink Surveillance Impact Report.

[2] This list represents all agencies who are able to see OPD data. These agencies do not actually necessarily see OPD data; OPD data only comes up in a search result list if something in the record has the same terms as those that a user puts into the search box. The further away from the location of the incident, an OPD record is unlikely to be in the top few results pages unless the exact person is found.

I. Training: *The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology;*

OPD's IT Unit shall ensure the development of training regarding authorized system use and access.

J. Auditing and Oversight: *The mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy; and*

The OPD IT Unit will manage audit requests in conjunction with Forensic Logic, Inc.

Per FBI CJIS Security Policy, Paragraph 5.4, Forensic Logic logs information about the following events and content and a report can be produced upon request at any time.

5.4.1.1 Events

The following events shall be logged:

1. Successful and unsuccessful system log-on attempts.
2. Successful and unsuccessful attempts to use:
    a. access permission on a user account, file, directory or other system resource;
    b. create permission on a user account, file, directory or other system resource;
    c. write permission on a user account, file, directory or other system resource;
    d. delete permission on a user account, file, directory or other system resource;
    e. change permission on a user account, file, directory or other system resource.
3. Successful and unsuccessful attempts to change account passwords.
4. Successful and unsuccessful actions by privileged accounts.
5. Successful and unsuccessful attempts for users to:
    a. access the audit log file;
    b. modify the audit log file;
    c. destroy the audit log file.

5.4.1.1.1 Content

The following content shall be included with every audited event:

1. Date and time of the event.
2. The component of the information system (e.g., software component, hardware component) where the event occurred.

3. Type of event.
4. User/subject identity.
5. Outcome (success or failure) of the event.

OPD's IT Unit shall provide the Chief of Police, Privacy Advisory Commission, and City Council with an annual report that covers use of Forensic Logic's CopLink and Crime Reporting modules during the previous year. The report shall include all report components compliant with Ordinance No. 13489 C.M.S.

K. Maintenance: *The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.*

Forensic Logic, Inc. shall be responsible for all system maintenance per the OPD-Forensic Logic, Inc "software as a service" or (SAAS) contract model.

By Order of

Susan E. Manheimer

Chief of Police Date Signed:

EXHIBIT E

CITY OF OAKLAND

MEMORANDUM

TO: PAC

FROM: Yun Zhou, Sergeant of Police
OPD, Criminal Investigation Division

SUBJECT: Forensic Logic CopLink / CrimeTracer System – 2024 Annual Report

DATE: May 12, 2025

Background

Oakland Municipal Code (OMC) 9.64.040: Surveillance Technology "Oversight following City Council approval" requires that for each approved surveillance technology item, City staff must present a written annual surveillance report for Privacy Advisory Commission (PAC). After review by the PAC, City staff shall submit the annual surveillance report to the City Council. The PAC shall recommend to the City Council that:

- The benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded.
- That use of the surveillance technology cease; or
- Propose modifications to the corresponding surveillance use policy that will resolve the concerns.

Oakland Police Department (OPD) Department General Order (DGO) I-24: Forensic Logic CopLink / LEAP, as well as OMC 9.64.040 together require that OPD provide an annual report to the Chief of Police, the PAC, and Public Safety Committee. The information provided below is compliant with these annual report requirements.

DGO I-24 explains that authorized members may use CopLink for the purpose of searching the system in the service of conducting criminal investigations, such as apprehending subjects, locating and returning stolen property, as well as in the protection of the law enforcement officers encountering the individuals described in the system. Authorized purposes also include other appropriate OPD organizational investigations (e.g., internal affairs, missing persons, and use of force investigations).

In 2023, CrimeTracer was introduced as the next iteration of CopLink. Forensic Logic also rebranded to SoundThinking. The product being used by OPD is now called SoundThinking CrimeTracer. OPD began migrating its user accounts in August of 2023 from CopLink to CrimeTracer. Functionally, it is the same product and consists of the same features and security. The only change made to the product is the name, logo and color scheme. Since the 2023 Annual Report, OPD has referred to the product as CrimeTracer.

Captain Nicholas Calonge, Criminal Investigation Division Commander, was the Program Coordinator for 2024.

A. **A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology**

CrimeTracer search technology is used regularly by both OPD sworn field / patrol personnel and command staff. Search parameters include the following criteria which are submitted to a search engine where data originating from law enforcement records, calls for service, field interviews, arrest/booking records and citations are stored:

- License plate numbers
- Persons of interest
- Locations
- Vehicle descriptions
- Incident numbers
- Offense descriptions/penal codes
- Geographic regions (e.g., Police Beats or Police Areas)

Data is stored in an FBI Criminal Justice Information Service (CJIS) compliant repository in the Microsoft Azure GovCloud.

In 2024, there were a total of 423 users accounts who conducted Forensic Logic searches, for a total of 204,750 separate queries. Table below breaks down this search data by month and by distinct user and total searches.

Table 1: OPD CrimeTracer Searches; by Distinct User and Search Totals – 2024

CrimeTracer

Search Type	***January***	***February***	***March***	***April***	***May***	***June***
Number of OPD distinct users in each month	*174*	*234*	*258*	*255*	*263*	*276*
Number of searches conducted	*15,068*	*15,838*	*17,104*	*17,386*	*20,604*	*18,278*

Search Type	***July***	***August***	***September***	***October***	***November***	***December***
Number of OPD distinct users in each month	*282*	*268*	*253*	*214*	*196*	*200*
Number of searches conducted	*19,756*	*19,443*	*18,521*	*16,646*	*12,563*	*13,543*

B. **Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):**

Data searched with the CrimeTracer system is entirely acquired from incident reports, citations, calls for service and field interviews that have already been recorded in originating Records Management Systems, Computer Aided Dispatch Systems, and Mobile Field Reporting Systems – from both OPD systems as well as from other law enforcement agency systems (other SoundThinking client agencies). The data is collected from OPD systems at least once every 24 hours; once the data is collected and resides in the SoundThinking

cloud repository, it is made available to agencies subscribing to the service who are permitted by their agency command staff to access CJIS information.

CrimeTracer does not keep statistics on who searched and viewed the data shared, but the system can be audited for a specific search.

Data sourced from the Oakland Police Department cannot be accessed by US DHS ICE nor US DHS CBP staff. Some federal agencies are using CrimeTracer with a limited licensing, meaning not every agents in the agency have access to CrimeTracer but the logins are assigned to various Federal Agents. These agencies are FBI, ATF, DEA, USPS, US Marshal and Secret Service.

Beyond federal access, CrimeTracer data is shared regionally with partner law enforcement agencies. Recipients include police departments, sheriff's offices, and state agencies across the following jurisdictions:

Los Angeles County, and agencies across Orange, San Bernardino, and Ventura counties

Santa Clara, Santa Cruz, Monterey, and San Benito counties, as well as agencies across San Francisco, San Mateo, Alameda, San Joaquin, Stanislaus, San Diego, and Fresno counties

State of Tennessee

State of Massachusetts

Maricopa, Pima, Pinal, and Yavapai counties in Arizona

Greater Kansas City region

Fulton and Cobb counties, Georgia

West and Central Oregon agencies

Spokane County, Washington

Reno, Sparks, and Washoe County, Nevada

El Paso and Houston, Texas

C. **Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to**

The CrimeTracer service is a web portal accessible by authorized OPD users on OPD computers with an appropriate user-id and password (criteria for both defined by FBI CJIS Security Addendum). OPD data sources that provide data accessible to the search tool include the following:

- Arrest records
- Field contacts

- Incident reports
- Service calls
- ShotSpotter Activations
- Stop Data reports
- Traffic Accident reports

D. **Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year**

Not applicable. The technology is a web portal that is accessible to computers on the OPD network.

E. **A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The PAC may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the PAC makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review.**

No community complaints or concerns were communicated to staff in 2024.

OPD is not able to provide the race of each person connected to each query. The technology is intended as a search engine of records (section C), not all queries would contain the race data of the person subject to the technology's use. OPD would have to individually evaluate tens of thousands of searches to provide the requested race data. Staff recommends the PAC makes the determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information.

F. **The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information**

No internal audit was conducted on CrimeTracer in 2024.

Staff was not made aware of any criminal or administrative investigation pertaining to the misuse of the technology in 2024.

G. **Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response**

There were no identifiable data breaches or known unauthorized access during 2024.

H. **Information, including case examples, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes:**

Homicide Case Examples

During the investigation of a homicide in the first quarter of 2024, the investigator searched CrimeTracer for prior incident reports involving the victim. One report detailed a recent argument involving the victim and another individual. A further search of field contact data showed the same individual had been contacted in the vicinity of the homicide scene days prior. This individual was later identified as the suspect and arrested.

During the investigation of a homicide in the third quarter of 2024, officers recovered a vehicle description from a witness. A CrimeTracer search of traffic accident reports found a recent collision involving a matching vehicle. The listed driver had prior arrests for firearm-related offenses. Further searches linked the driver to the scene, and the individual later identified as the homicide suspect.

Shooting Case Example

During the investigation of a shooting in the second quarter of 2024, the investigator reviewed prior ShotSpotter activations near the scene. A CrimeTracer search of field contacts within the activation radius showed an individual stopped minutes after a prior incident. That individual matched the description of the suspect provided by a witness. A review of prior arrests confirmed a history of gun-related charges. This information assisted in proving this individual to be the shooting suspect.

Burglary Case Examples

During the investigation of a residential burglary in the second quarter of 2024, officers identified a unique item stolen from the scene. A search in CrimeTracer showed a recent field contact where the same item was described in the narrative in the possession of a particular individual. Investigators followed up and later arrested the individual for the burglary.

Robbery Case Example

In the first quarter of 2024, patrol officers responded to a robbery where the suspect fled in a vehicle. The license plate was provided by a witness. A CrimeTracer search located a recent contact report involving the vehicle. One of the listed occupants had multiple prior arrests for robbery and was wearing clothing matching the description given by the victim. That individual was eventually arrested for the robbery.

I. **Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates**

There are no existing or newly opened public records requests relating to the technology.

J. **Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year**

Description		Amount
Contract Start Date 7/1/2025	**Contract End Date** 6/30/2026	
197-0000-04 CrimeTracer	CrimeTracer Enterprise Subscription for Term 7/1/2025-6/30/2026	$227,500.00
197-0000-04 CrimeTracer	COPLINIK Connect	$10,000.00
197-0000-04 CrimeTracer	CompStat, per user subscription (60 users @ $1,000 each)	$0.00
197-0000-04 CrimeTracer	General Purpose and Maintenance Services	$25,000.00
	Total	**$262,500.00**

K. **Any requested modifications to the Surveillance Use Policy and a detailed basis for the request**

No requests for changes at this time.

EXHIBIT F

Senate Bill No. 34

CHAPTER 532

An act to amend Sections 1798.29 and 1798.82 of, and to add Title 1.81.23 (commencing with Section 1798.90.5) to Part 4 of Division 3 of, the Civil Code, relating to personal information.

[Approved by Governor October 6, 2015. Filed with Secretary of State October 6, 2015.]

LEGISLATIVE COUNSEL'S DIGEST

SB 34, Hill. Automated license plate recognition systems: use of data.

(1) Existing law authorizes the Department of the California Highway Patrol to retain license plate data captured by license plate recognition (LPR) technology, also referred to as an automated license plate recognition (ALPR) system, for not more than 60 days unless the data is being used as evidence or for the investigation of felonies. Existing law prohibits the department from selling the data or from making the data available to an agency that is not a law enforcement agency or an individual that is not a law enforcement officer.

Existing law authorizes the department to use LPR data for the purpose of locating vehicles or persons reasonably suspected of being involved in the commission of a public offense, and requires the department to monitor the internal use of the data to prevent unauthorized use and to submit to the Legislature, as a part of the annual automobile theft report, information on the department's LPR practices and usage.

This bill would impose specified requirements on an "ALPR operator" as defined, including, among others, maintaining reasonable security procedures and practices to protect ALPR information and implementing a usage and privacy policy with respect to that information, as specified. The bill would impose similar requirements on an "ALPR end-user," as defined.

The bill would require an ALPR operator that accesses or provides access to ALPR information to maintain a specified record of that access and require that ALPR information only be used for authorized purposes.

The bill would, in addition to any other sanctions, penalties, or remedies provided by law, authorize an individual who has been harmed by a violation of these provisions to bring a civil action in any court of competent jurisdiction against a person who knowingly caused the harm.

The bill would require a public agency, as defined, that operates or intends to operate an ALPR system to provide an opportunity for public comment at a regularly scheduled public meeting of the governing body of the public agency before implementing the program. The bill would also prohibit a public agency from selling, sharing, or transferring ALPR information, except to another public agency, as specified.

(2) Existing law requires any agency, and any person or business conducting business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the system or data, as defined, following discovery or notification of the security breach, to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Existing law defines "personal information" for these purposes to include an individual's first name and last name, or first initial and last name, in combination with one or more designated data elements relating to, among other things, social security numbers, driver's license numbers, financial accounts, and medical information.

This bill would include information or data collected through the use or operation of an automated license plate recognition system, when that information is not encrypted and is used in combination with an individual's name, in the definition of "personal information" discussed above.

This bill would incorporate additional changes to Section 1798.29 of the Civil Code proposed by SB 570 and AB 964 that would become operative if this bill and one or both of those bills are enacted and this bill is enacted last.

This bill also would incorporate additional changes to Section 1798.82 of the Civil Code proposed by SB 570 and AB 964 that would become operative if this bill and one or both of those bills are enacted and this bill is enacted last.

The people of the State of California do enact as follows:

SECTION 1. Section 1798.29 of the Civil Code is amended to read:

1798.29. (a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after

the law enforcement agency determines that it will not compromise the investigation.

(d) Any agency that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language.

(2) The security breach notification shall include, at a minimum, the following information:

(A) The name and contact information of the reporting agency subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

(D) Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a social security number or a driver's license or California identification card number.

(3) At the discretion of the agency, the security breach notification may also include any of the following:

(A) Information about what the agency has done to protect individuals whose information has been breached.

(B) Advice on steps that the person whose information has been breached may take to protect himself or herself.

(4) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (g) for an online account, and no other personal information defined in paragraph (1) of subdivision (g), the agency may comply with this section by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the agency and all other online accounts for which the person uses the same user name or email address and password or security question or answer.

(5) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (g) for login credentials of an email account furnished by the agency, the agency shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in subdivision (i) or by clear and conspicuous notice delivered to the resident online when the resident is connected to the

online account from an Internet Protocol address or online location from which the agency knows the resident customarily accesses the account.

(e) Any agency that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

(f) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(g) For purposes of this section, "personal information" means either of the following:

(1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(A) Social security number.

(B) Driver's license number or California identification card number.

(C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(D) Medical information.

(E) Health insurance information.

(F) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.

(2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(h) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(i) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) Email notice when the agency has an email address for the subject persons.

(B) Conspicuous posting of the notice on the agency's Internet Web site page, if the agency maintains one.

(C) Notification to major statewide media and the Office of Information Security within the Department of Technology.

(j) Notwithstanding subdivision (i), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

(k) Notwithstanding the exception specified in paragraph (4) of subdivision (b) of Section 1798.3, for purposes of this section, "agency" includes a local agency, as defined in subdivision (a) of Section 6252 of the Government Code.

SEC. 1.1. Section 1798.29 of the Civil Code is amended to read:

1798.29. (a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) Any agency that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described in paragraph (2) under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

(A) The format of the notice shall be designed to call attention to the nature and significance of the information it contains.

(B) The title and headings in the notice shall be clearly and conspicuously displayed.

(C) The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.

(D) For a written notice described in paragraph (1) of subdivision (i), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

[NAME OF INSTITUTION / LOGO]	Date: [insert date]
NOTICE OF DATA BREACH	
What Happened?	
What Information Was Involved?	
What We Are Doing.	
What You Can Do.	

Other Important Information. [insert other important information]	
For More Information.	Call [telephone number] or go to [Internet Web site]

(E) For an electronic notice described in paragraph (2) of subdivision (i), use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

(2) The security breach notification described in paragraph (1) shall include, at a minimum, the following information:

(A) The name and contact information of the reporting agency subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

(D) Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a social security number or a driver's license or California identification card number.

(3) At the discretion of the agency, the security breach notification may also include any of the following:

(A) Information about what the agency has done to protect individuals whose information has been breached.

(B) Advice on steps that the person whose information has been breached may take to protect himself or herself.

(e) Any agency that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

(f) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(g) For purposes of this section, "personal information" means either of the following:

(1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(A) Social security number.

(B) Driver's license number or California identification card number.

(C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(D) Medical information.

(E) Health insurance information.

(F) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.

(2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(h) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(i) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) Email notice when the agency has an email address for the subject persons.

(B) Conspicuous posting, for a minimum of 30 days, of the notice on the agency's Internet Web site page, if the agency maintains one. For purposes of this subparagraph, conspicuous posting on the agency's Internet Web site means providing a link to the notice on the home page or first significant page after entering the Internet Web site that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link.

(C) Notification to major statewide media and the Office of Information Security within the Department of Technology.

(4) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (g) for an online account, and no other personal information defined in paragraph (1) of subdivision (g), the agency may comply with this section by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the agency and all other online accounts for which the person uses the same user name or email address and password or security question or answer.

(5) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (g) for login credentials of an email account furnished by the agency, the agency shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in this subdivision or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the agency knows the resident customarily accesses the account.

(j) Notwithstanding subdivision (i), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

(k) Notwithstanding the exception specified in paragraph (4) of subdivision (b) of Section 1798.3, for purposes of this section, "agency" includes a local agency, as defined in subdivision (a) of Section 6252 of the Government Code.

SEC. 1.2. Section 1798.29 of the Civil Code is amended to read:

1798.29. (a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) Any agency that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language.

(2) The security breach notification shall include, at a minimum, the following information:

(A) The name and contact information of the reporting agency subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

(D) Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a social security number or a driver’s license or California identification card number.

(3) At the discretion of the agency, the security breach notification may also include any of the following:

(A) Information about what the agency has done to protect individuals whose information has been breached.

(B) Advice on steps that the person whose information has been breached may take to protect himself or herself.

(4) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (g) for an online account, and no other personal information defined in paragraph (1) of subdivision (g), the agency may comply with this section by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the agency and all other online accounts for which the person uses the same user name or email address and password or security question or answer.

(5) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (g) for login credentials of an email account furnished by the agency, the agency shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in subdivision (i) or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the agency knows the resident customarily accesses the account.

(e) Any agency that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

(f) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(g) For purposes of this section, "personal information" means either of the following:

(1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(A) Social security number.

(B) Driver's license number or California identification card number.

(C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(D) Medical information.

(E) Health insurance information.

(F) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.

(2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(h) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(4) For purposes of this section, "encrypted" means rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.

(i) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) Email notice when the agency has an email address for the subject persons.

(B) Conspicuous posting of the notice on the agency's Internet Web site page, if the agency maintains one.

(C) Notification to major statewide media and the Office of Information Security within the Department of Technology.

(j) Notwithstanding subdivision (i), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

(k) Notwithstanding the exception specified in paragraph (4) of subdivision (b) of Section 1798.3, for purposes of this section, "agency" includes a local agency, as defined in subdivision (a) of Section 6252 of the Government Code.

SEC. 1.3. Section 1798.29 of the Civil Code is amended to read:

1798.29. (a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of

the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) Any agency that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described in paragraph (2) under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

(A) The format of the notice shall be designed to call attention to the nature and significance of the information it contains.

(B) The title and headings in the notice shall be clearly and conspicuously displayed.

(C) The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.

(D) For a written notice described in paragraph (1) of subdivision (i), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

[NAME OF INSTITUTION / LOGO]	Date: [insert date]
NOTICE OF DATA BREACH	
What Happened?	

What Information Was Involved?	
What We Are Doing.	
What You Can Do.	
Other Important Information. [insert other important information]	
For More Information.	Call [telephone number] or go to [Internet Web site]

(E) For an electronic notice described in paragraph (2) of subdivision (i), use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

(2) The security breach notification described in paragraph (1) shall include, at a minimum, the following information:

(A) The name and contact information of the reporting agency subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

(D) Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a social security number or a driver's license or California identification card number.

(3) At the discretion of the agency, the security breach notification may also include any of the following:

(A) Information about what the agency has done to protect individuals whose information has been breached.

(B) Advice on steps that the person whose information has been breached may take to protect himself or herself.

(e) Any agency that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

(f) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(g) For purposes of this section, "personal information" means either of the following:

(1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(A) Social security number.

(B) Driver's license number or California identification card number.

(C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(D) Medical information.

(E) Health insurance information.

(F) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.

(2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(h) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(4) For purposes of this section, "encrypted" means rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.

(i) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) Email notice when the agency has an email address for the subject persons.

(B) Conspicuous posting, for a minimum of 30 days, of the notice on the agency's Internet Web site page, if the agency maintains one. For purposes of this subparagraph, conspicuous posting on the agency's Internet Web site means providing a link to the notice on the home page or first significant page after entering the Internet Web site that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link.

(C) Notification to major statewide media and the Office of Information Security within the Department of Technology.

(4) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (g) for an online account, and no other personal information defined in paragraph (1) of subdivision (g), the agency may comply with this section by providing the security breach notification in electronic or other form that directs the person whose

personal information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the agency and all other online accounts for which the person uses the same user name or email address and password or security question or answer.

(5) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (g) for login credentials of an email account furnished by the agency, the agency shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in this subdivision or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the agency knows the resident customarily accesses the account.

(j) Notwithstanding subdivision (i), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

(k) Notwithstanding the exception specified in paragraph (4) of subdivision (b) of Section 1798.3, for purposes of this section, "agency" includes a local agency, as defined in subdivision (a) of Section 6252 of the Government Code.

SEC. 2. Section 1798.82 of the Civil Code is amended to read:

1798.82. (a) A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.

(d) A person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language.

(2) The security breach notification shall include, at a minimum, the following information:

(A) The name and contact information of the reporting person or business subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

(D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.

(G) If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months, along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information defined in subparagraphs (A) and (B) of paragraph (1) of subdivision (h).

(3) At the discretion of the person or business, the security breach notification may also include any of the following:

(A) Information about what the person or business has done to protect individuals whose information has been breached.

(B) Advice on steps that the person whose information has been breached may take to protect himself or herself.

(4) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (h) for an online account, and no other personal information defined in paragraph (1) of subdivision (h), the person or business may comply with this section by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached promptly to change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same user name or email address and password or security question or answer.

(5) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (h) for login credentials of an email account furnished by the person or business, the person or business shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in subdivision (j) or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the person or business knows the resident customarily accesses the account.

(e) A covered entity under the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d et seq.) will be deemed to have complied with the notice requirements in subdivision (d) if it has complied completely with Section 13402(f) of the federal Health Information Technology for Economic and Clinical Health Act (Public Law 111-5). However, nothing in this subdivision shall be construed to exempt a covered entity from any other provision of this section.

(f) A person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

(g) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(h) For purposes of this section, "personal information" means either of the following:

(1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(A) Social security number.

(B) Driver's license number or California identification card number.

(C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(D) Medical information.

(E) Health insurance information.

(F) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.

(2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(i) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(j) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) Email notice when the person or business has an email address for the subject persons.

(B) Conspicuous posting of the notice on the Internet Web site page of the person or business, if the person or business maintains one.

(C) Notification to major statewide media.

(k) Notwithstanding subdivision (j), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

SEC. 2.1. Section 1798.82 of the Civil Code is amended to read:

1798.82. (a) A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify

the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.

(d) A person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described in paragraph (2) under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

(A) The format of the notice shall be designed to call attention to the nature and significance of the information it contains.

(B) The title and headings in the notice shall be clearly and conspicuously displayed.

(C) The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.

(D) For a written notice described in paragraph (1) of subdivision (j), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

[NAME OF INSTITUTION / LOGO]	Date: [insert date]
NOTICE OF DATA BREACH	
What Happened?	
What Information Was Involved?	

What We Are Doing.	
What You Can Do.	
Other Important Information. [insert other important information]	
For More Information.	Call [telephone number] or go to [Internet Web site]

(E) For an electronic notice described in paragraph (2) of subdivision (j), use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

(2) The security breach notification described in paragraph (1) shall include, at a minimum, the following information:

(A) The name and contact information of the reporting person or business subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

(D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.

(G) If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information defined in subparagraphs (A) and (B) of paragraph (1) of subdivision (h).

(3) At the discretion of the person or business, the security breach notification may also include any of the following:

(A) Information about what the person or business has done to protect individuals whose information has been breached.

(B) Advice on steps that the person whose information has been breached may take to protect himself or herself.

(e) A covered entity under the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d et seq.) will be deemed to have complied with the notice requirements in subdivision (d) if it has complied completely with Section 13402(f) of the federal Health Information Technology for Economic and Clinical Health Act (Public Law 111-5). However, nothing in this subdivision shall be construed to exempt a covered entity from any other provision of this section.

(f) A person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

(g) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(h) For purposes of this section, "personal information" means either of the following:

(1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(A) Social security number.

(B) Driver's license number or California identification card number.

(C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(D) Medical information.

(E) Health insurance information.

(F) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.

(2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(i) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(j) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) Email notice when the person or business has an email address for the subject persons.

(B) Conspicuous posting, for a minimum of 30 days, of the notice on the Internet Web site page of the person or business, if the person or business maintains one. For purposes of this subparagraph, conspicuous posting on the person's or business's Internet Web site means providing a link to the notice on the home page or first significant page after entering the Internet Web site that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link.

(C) Notification to major statewide media.

(4) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (h) for an online account, and no other personal information defined in paragraph (1) of subdivision (h), the person or business may comply with this section by providing the

security breach notification in electronic or other form that directs the person whose personal information has been breached promptly to change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same user name or email address and password or security question or answer.

(5) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (h) for login credentials of an email account furnished by the person or business, the person or business shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in this subdivision or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the person or business knows the resident customarily accesses the account.

(k) Notwithstanding subdivision (j), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

SEC. 2.2. Section 1798.82 of the Civil Code is amended to read:

1798.82. (a) A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.

(d) A person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language.

(2) The security breach notification shall include, at a minimum, the following information:

(A) The name and contact information of the reporting person or business subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

(D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.

(G) If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months, along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information defined in subparagraphs (A) and (B) of paragraph (1) of subdivision (h).

(3) At the discretion of the person or business, the security breach notification may also include any of the following:

(A) Information about what the person or business has done to protect individuals whose information has been breached.

(B) Advice on steps that the person whose information has been breached may take to protect himself or herself.

(4) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (h) for an online account, and no other personal information defined in paragraph (1) of subdivision (h), the person or business may comply with this section by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached promptly to change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same user name or email address and password or security question or answer.

(5) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (h) for login credentials of an email account furnished by the person or business, the person or business shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in subdivision (j) or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the person or business knows the resident customarily accesses the account.

(e) A covered entity under the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d et seq.) will be deemed to have complied with the notice requirements in subdivision (d) if it has complied completely with Section 13402(f) of the federal Health Information Technology for Economic and Clinical Health Act (Public Law 111-5). However, nothing in this subdivision shall be construed to exempt a covered entity from any other provision of this section.

(f) A person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

(g) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(h) For purposes of this section, "personal information" means either of the following:

(1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(A) Social security number.

(B) Driver's license number or California identification card number.

(C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(D) Medical information.

(E) Health insurance information.

(F) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.

(2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(i) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(4) For purposes of this section, "encrypted" means rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.

(j) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) Email notice when the person or business has an email address for the subject persons.

(B) Conspicuous posting of the notice on the Internet Web site page of the person or business, if the person or business maintains one.

(C) Notification to major statewide media.

(k) Notwithstanding subdivision (j), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

SEC. 2.3. Section 1798.82 of the Civil Code is amended to read:

1798.82. (a) A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided

in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.

(d) A person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described in paragraph (2) under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

(A) The format of the notice shall be designed to call attention to the nature and significance of the information it contains.

(B) The title and headings in the notice shall be clearly and conspicuously displayed.

(C) The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.

(D) For a written notice described in paragraph (1) of subdivision (j), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

[NAME OF INSTITUTION / LOGO]	Date: [insert date]
NOTICE OF DATA BREACH	
What Happened?	

What Information Was Involved?	
What We Are Doing.	
What You Can Do.	
Other Important Information. [insert other important information]	
For More Information.	Call [telephone number] or go to [Internet Web site]

(E) For an electronic notice described in paragraph (2) of subdivision (j), use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

(2) The security breach notification described in paragraph (1) shall include, at a minimum, the following information:

(A) The name and contact information of the reporting person or business subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

(D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.

(G) If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information defined in subparagraphs (A) and (B) of paragraph (1) of subdivision (h).

(3) At the discretion of the person or business, the security breach notification may also include any of the following:

(A) Information about what the person or business has done to protect individuals whose information has been breached.

(B) Advice on steps that the person whose information has been breached may take to protect himself or herself.

(e) A covered entity under the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d et seq.) will be deemed to have complied with the notice requirements in subdivision (d) if it has complied completely with Section 13402(f) of the federal Health Information Technology for Economic and Clinical Health Act (Public Law 111-5). However, nothing in this subdivision shall be construed to exempt a covered entity from any other provision of this section.

(f) A person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

(g) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(h) For purposes of this section, "personal information" means either of the following:

(1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(A) Social security number.

(B) Driver's license number or California identification card number.

(C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(D) Medical information.

(E) Health insurance information.

(F) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.

(2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(i) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(4) For purposes of this section, "encrypted" means rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.

(j) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) Email notice when the person or business has an email address for the subject persons.

(B) Conspicuous posting, for a minimum of 30 days, of the notice on the Internet Web site page of the person or business, if the person or business maintains one. For purposes of this subparagraph, conspicuous posting on the person's or business's Internet Web site means providing a link to the notice on the home page or first significant page after entering the Internet

Web site that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link.

(C) Notification to major statewide media.

(4) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (h) for an online account, and no other personal information defined in paragraph (1) of subdivision (h), the person or business may comply with this section by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached promptly to change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same user name or email address and password or security question or answer.

(5) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (h) for login credentials of an email account furnished by the person or business, the person or business shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in this subdivision or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the person or business knows the resident customarily accesses the account.

(k) Notwithstanding subdivision (j), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

SEC. 3. Title 1.81.23 (commencing with Section 1798.90.5) is added to Part 4 of Division 3 of the Civil Code, to read:

TITLE 1.81.23. COLLECTION OF LICENSE PLATE INFORMATION

1798.90.5. The following definitions shall apply for purposes of this title:

(a) “Automated license plate recognition end-user” or “ALPR end-user” means a person that accesses or uses an ALPR system, but does not include any of the following:

(1) A transportation agency when subject to Section 31490 of the Streets and Highways Code.

(2) A person that is subject to Sections 6801 to 6809, inclusive, of Title 15 of the United States Code and state or federal statutes or regulations implementing those sections, if the person is subject to compliance oversight by a state or federal regulatory agency with respect to those sections.

(3) A person, other than a law enforcement agency, to whom information may be disclosed as a permissible use pursuant to Section 2721 of Title 18 of the United States Code.

(b) "Automated license plate recognition information," or "ALPR information" means information or data collected through the use of an ALPR system.

(c) "Automated license plate recognition operator" or "ALPR operator" means a person that operates an ALPR system, but does not include a transportation agency when subject to Section 31490 of the Streets and Highways Code.

(d) "Automated license plate recognition system" or "ALPR system" means 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 of registration plates and the characters they contain into computer-readable data.

(e) "Person" means any natural person, public agency, partnership, firm, association, corporation, limited liability company, or other legal entity.

(f) "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.

1798.90.51. An ALPR operator shall do all of the following:

(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 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.

1798.90.52. If an ALPR operator accesses or provides access to ALPR information, the ALPR operator shall do both of the following:

(a) Maintain a record of that access. At a minimum, the record shall include all of the following:

(1) The date and time the information is accessed.

(2) The license plate number or other data elements used to query the ALPR system.

(3) The username of the person who accesses the information, and, as applicable, the organization or entity with whom the person is affiliated.

(4) The purpose for accessing the information.

(b) Require that ALPR information only be used for the authorized purposes described in the usage and privacy policy required by subdivision (b) of Section 1798.90.51.

1798.90.53. An ALPR end-user shall do all of the following:

(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 ALPR information.

(B) A description of the job title or other designation of the employees and independent contractors who are authorized to access and use 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 all 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 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.

1798.90.54. (a) In addition to any other sanctions, penalties, or remedies provided by law, an individual who has been harmed by a violation of this title, including, but not limited to, unauthorized access or use of ALPR information or a breach of security of an ALPR system, may bring a civil action in any court of competent jurisdiction against a person who knowingly caused the harm.

(b) The court may award a combination of any one or more of the following:

(1) Actual damages, but not less than liquidated damages in the amount of two thousand five hundred dollars ($2,500).

(2) Punitive damages upon proof of willful or reckless disregard of the law.

(3) Reasonable attorney's fees and other litigation costs reasonably incurred.

(4) Other preliminary and equitable relief as the court determines to be appropriate.

1798.90.55. Notwithstanding any other law or regulation:

(a) A public agency that operates or intends to operate an ALPR system shall provide an opportunity for public comment at a regularly scheduled public meeting of the governing body of the public agency before implementing the program.

(b) A public agency shall not sell, share, or transfer ALPR information, except to another public agency, and only as otherwise permitted by law. For purposes of this section, the provision of data hosting or towing services shall not be considered the sale, sharing, or transferring of ALPR information.

SEC. 4. (a) Section 1.1 of this bill incorporates amendments to Section 1798.29 of the Civil Code proposed by both this bill and Senate Bill 570. It shall only become operative if (1) both bills are enacted and become effective on or before January 1, 2016, (2) each bill amends Section 1798.29 of the Civil Code, (3) Assembly Bill 964 is not enacted or as enacted does not amend that section, and (4) this bill is enacted after Senate Bill 570, in which case Sections 1, 1.2, and 1.3 of this bill shall not become operative.

(b) Section 1.2 of this bill incorporates amendments to Section 1798.29 of the Civil Code proposed by both this bill and Assembly Bill 964. It shall only become operative if (1) both bills are enacted and become effective on or before January 1, 2016, (2) each bill amends Section 1798.29 of the Civil Code, (3) Senate Bill 570 is not enacted or as enacted does not amend that section, and (4) this bill is enacted after Assembly Bill 964, in which case Sections 1, 1.1, and 1.3 of this bill shall not become operative.

(c) Section 1.3 of this bill incorporates amendments to Section 1798.29 of the Civil Code proposed by this bill, Senate Bill 570, and Assembly Bill

964. It shall only become operative if (1) all three bills are enacted and become effective on or before January 1, 2016, (2) all three bills amend Section 1798.29 of the Civil Code, and (3) this bill is enacted after Senate Bill 570 and Assembly Bill 964, in which case Sections 1, 1.1, and 1.2 of this bill shall not become operative.

SEC. 5. (a) Section 2.1 of this bill incorporates amendments to Section 1798.82 of the Civil Code proposed by both this bill and Senate Bill 570. It shall only become operative if (1) both bills are enacted and become effective on or before January 1, 2016, (2) each bill amends Section 1798.82 of the Civil Code, (3) Assembly Bill 964 is not enacted or as enacted does not amend that section, and (4) this bill is enacted after Senate Bill 570, in which case Sections 2, 2.2, and 2.3 of this bill shall not become operative.

(b) Section 2.2 of this bill incorporates amendments to Section 1798.82 of the Civil Code proposed by both this bill and Assembly Bill 964. It shall only become operative if (1) both bills are enacted and become effective on or before January 1, 2016, (2) each bill amends Section 1798.82 of the Civil Code, (3) Senate Bill 570 is not enacted or as enacted does not amend that section, and (4) this bill is enacted after Assembly Bill 964, in which case Sections 2, 2.1, and 2.3 of this bill shall not become operative.

(c) Section 2.3 of this bill incorporates amendments to Section 1798.82 of the Civil Code proposed by this bill, Senate Bill 570, and Assembly Bill 964. It shall only become operative if (1) all three bills are enacted and become effective on or before January 1, 2016, (2) all three bills amend Section 1798.82 of the Civil Code, and (3) this bill is enacted after Senate Bill 570 and Assembly Bill 964, in which case Sections 2, 2.1, and 2.2 of this bill shall not become operative.

O

EXHIBIT G

Automated License Plate Readers

To Better Protect Individuals' Privacy, Law Enforcement Must Increase Its Safeguards for the Data It Collects

February 2020

REPORT 2019-118

CALIFORNIA STATE AUDITOR
621 Capitol Mall, Suite 1200 | Sacramento | CA | 95814

916.445.0255 | TTY **916.445.0033**

For complaints of state employee misconduct,
contact us through the **Whistleblower Hotline**:
1.800.952.5665

Don't want to miss any of our reports? Subscribe to our email list at **auditor.ca.gov**

For questions regarding the contents of this report, please contact Margarita Fernández, Chief of Public Affairs, *at* 916.445.0255

Elaine M. Howle *State Auditor*

February 13, 2020
2019-118

The Governor of California
President pro Tempore of the Senate
Speaker of the Assembly
State Capitol
Sacramento, California 95814

Dear Governor and Legislative Leaders:

As directed by the Joint Legislative Audit Committee, my office conducted an audit of local law enforcement agencies' use of automated license plate readers (ALPR); the following report details the audit's findings and conclusions. In general, we determined that the law enforcement agencies we reviewed must better protect individuals' privacy through ensuring that their policies reflect state law. In addition, we found that these agencies must improve their ALPR data security, make more informed decisions about sharing their ALPR data, and expand their oversight of ALPR users.

We reviewed four agencies in detail that operate ALPR systems—Fresno Police Department, Los Angeles Police Department, Marin County Sheriff's Office, and Sacramento County Sheriff's Office. An ALPR system collects and stores license plate images of vehicles passing in its view and enables law enforcement to track a vehicle's movements over time; such a system raises privacy concerns. State law helps address these concerns by requiring agencies to have policies and safeguards in place to protect their ALPR systems from misuse. However, the agencies we reviewed either did not have ALPR policies or their policies were deficient, and they had not implemented sufficient safeguards. For example, none had audited searches of the ALPR images by their staff and thus had no assurance that the searches were appropriate. Furthermore, three of the four agencies have shared their ALPR images widely, without considering whether the entities receiving them have a right to and need for the images. The statewide survey of law enforcement agencies we conducted found that 70 percent operate or plan to operate an ALPR system, and this raises concerns that these agencies may share the deficiencies we identified at the four agencies we reviewed. Because many of the issues we identified link to the agencies' deficient ALPR policies we recommend that the Legislature direct the California Department of Justice to develop a policy template that local law enforcement agencies can use as a model for their ALPR policies.

Our statewide survey also showed that the period of time law enforcement agencies retain ALPR images varies widely. However, among the four agencies we reviewed none had considered the usefulness of the ALPR images to investigators over time when determining their retention periods. We recommend that the Legislature amend state law to specify a maximum retention period for ALPR images.

Respectfully submitted,

Elaine M. Howle

ELAINE M. HOWLE, CPA
California State Auditor

Selected Abbreviations Used in This Report

ACLU	American Civil Liberties Union
ALPR	Automated license plate reader
CHP	California Highway Patrol
CJIS	Criminal Justice Information Services Division
CLETS	California Law Enforcement Telecommunications System
FBI	Federal Bureau of Investigation
GPS	Global positioning system
ICE	U.S. Immigration and Customs Enforcement
IT	Information technology
OECD	Organization for Economic Cooperation and Development

Contents

Blank page inserted for reproduction purposes only.

Summary

Results in Brief

To better protect the privacy of residents, local law enforcement agencies must improve their policies, procedures, and monitoring for the use and retention of license plate images and corresponding data. The majority of California law enforcement agencies (agencies) collect and use images captured by automated license plate reader (ALPR) cameras. The ALPR system is both a real-time tool for these agencies and an archive of historical images. Fixed cameras mounted to stationary objects, such as light poles, and mobile cameras mounted to law enforcement vehicles, capture ALPR images. Software extracts the license plate number from the image and stores it, with the date, time, and location of the scan and sometimes a partial image of the vehicle, in a searchable database. The software also automatically compares the plate number to stored lists of vehicles of interest, called *hot lists* then issues alerts, called *hits* if the plate number matches an entry on the hot list. Agencies compile these hot lists based on vehicles sought in crime investigations and vehicles connected to people of interest—for example, a list of stolen vehicles or of missing persons. We use the term *ALPR data* to describe all the information stored in an ALPR system, including license plate images and hot lists.

Because an ALPR system stores the plate number and image in a database even if the plate number does not match one on a hot list, the American Civil Liberties Union (ACLU) raised concerns in a 2013 report about law enforcement collecting and storing ALPR images related to individuals not suspected of crimes. The ACLU noted that law enforcement officers could inappropriately monitor the movements of individuals such as ex-spouses, neighbors, and other associates—actions that do not respect individuals' privacy. Although ALPR supporters contend that the images are collected in public places where there is no reasonable expectation of privacy, state law has made privacy a consideration when operating or using an ALPR system. Nonetheless, we found that the handling and retention of ALPR images and associated data did not always follow practices that adequately consider an individual's privacy.

Although law enforcement agencies collect ALPR images in public view, and there is no reasonable expectation of privacy regarding a license plate, the use and retention of those images raises privacy concerns. The four local law enforcement agencies we reviewed—Fresno Police Department (Fresno), Los Angeles Police Department (Los Angeles), Marin County Sheriff's Office (Marin), and Sacramento County Sheriff's Office (Sacramento)—have accumulated a large number of images in their ALPR systems, yet most of these images are unrelated to their criminal investigations.

Audit Highlights . . .

Our audit of the use of automated license plate readers (ALPR) at four local law enforcement agencies highlighted the following:

» *Local law enforcement agencies did not always follow practices that adequately consider the individual's privacy in handling and retaining the ALPR images and associated data.*

» *All four agencies have accumulated a large number of images in their ALPR systems, yet most of the images do not relate to their criminal investigations—99.9 percent of the 320 million images Los Angeles stores are for vehicles that were not on a* hot list *when the image was made.*

- *None of the agencies have an ALPR usage and privacy policy that implements all the legally mandated—since 2016—requirements.*
- *Three agencies did not completely or clearly specify who has system access, who has system oversight, or how to destroy ALPR data, and the remaining agency has not developed a policy at all.*
- *Two of the agencies add and store names, addresses, dates of birth, and criminal charges to their systems—some of these data may be categorized as criminal justice information and may originate from a system maintained and protected by the Department of Justice.*

continued on next page . . .

- *Three agencies use a cloud storage vendor to hold their many images and associated data, yet the agencies lack contract guarantees that the cloud vendor will appropriately protect the data.*
- *Three agencies share their images with hundreds of entities across the U.S. but could not provide evidence that they had determined whether those entities have a right or a need to access the images.*

» *Agencies may be retaining the images longer than necessary and thus increasing the risk to individuals' privacy.*

» *The agencies have few safeguards for creating ALPR user accounts and have not audited the use of their systems.*

For example, at Los Angeles only 400,000 of the 320 million images it has accumulated over several years and stores in its database generated an immediate match against its hot lists. In other words, 99.9 percent of the ALPR images Los Angeles stores are for vehicles that were not on a hot list at the time the image was made. Nevertheless, the stored images provide value beyond immediate hit alerts, as law enforcement personnel can search the accumulated images to determine the vehicles present at particular locations and to track vehicles' movements at particular times in order to gather or resolve leads in investigations.

Technology gives governments the ability to accumulate volumes of information about people, raising a reasonable question: How is an individual's privacy to be preserved? Effective in 2016 the California Legislature addressed privacy with respect to ALPR systems through Senate Bill 34 (Statutes of 2015, Chapter 532) (SB 34) by establishing requirements for these systems, including requiring detailed usage and privacy policies that describe the system's purpose, who may use it, how the agency will share data, how the agency will protect and monitor the system, and how long the agency will keep the data. Yet the agencies we reviewed have not implemented all of the requirements in that law.

Law enforcement agencies must first create policies that set clear guidelines for how they will use ALPR data. Setting certain expectations in writing through an ALPR usage and privacy policy helps ensure that agencies operate their ALPR programs in a manner that better protects individuals' privacy. However, none of the four agencies have an ALPR policy that contains all of the required information. In fact, Los Angeles has not developed an ALPR policy at all. The other three agencies did not completely or clearly specify who has system access, who has system oversight, or how to destroy ALPR data. Their poorly developed and incomplete policies contributed to the agencies' failure to implement ALPR programs that reflect the privacy principles in SB 34.

ALPR systems may contain data beyond license plate images. For example, we found that Sacramento and Los Angeles are adding names, addresses, dates of birth, and criminal charges to their ALPR systems, which are then stored in those systems. Some of these data may be categorized as criminal justice information; in addition, the data may originate from the California Law Enforcement Telecommunications System (CLETS), which the California Department of Justice (Justice) maintains. These various types of data require different levels of protection under the law. State law requires these agencies to maintain reasonable security procedures and practices to protect ALPR data from unauthorized access, destruction, use, modification, or disclosure. In addition, we believe that policy from the Criminal Justice Information Services

Division (CJIS) of the U.S. Federal Bureau of Investigation (FBI) models reasonable security measures for law enforcement agencies' ALPR data. CJIS policy specifies operational, administrative, technical, and physical safeguards for each of the areas specified in state law.

Fresno, Marin, and Sacramento use a cloud storage solution to hold their many ALPR images and associated data. Although the three agencies told us their systems comply with CJIS policy, none of them could demonstrate the vetting they performed to confirm that their cloud storage vendor did, in fact, meet the CJIS policy standards. Moreover, none of the contracts these three agencies have with their cloud storage vendors include all necessary data security safeguards. Thus, the agencies lack guarantees that the cloud vendor will provide appropriate protection of their data.

Law enforcement agencies of all types may benefit from guidance to improve their policies and data security practices. We surveyed 391 police and sheriff departments statewide, and of those using an ALPR system, 96 percent stated that they have ALPR policies, and nearly all reported that their ALPR data storage solution complies with CJIS policy. However, it is likely that many of the survey respondents have the same problems we identified at the four agencies we visited. Justice has experience guiding law enforcement agencies to help them adhere to state law and to improve their administrative practices. By developing guidance for local agencies on needed ALPR policy elements, Justice could help them improve the quality and completeness of their policies.

State law allows law enforcement agencies to share ALPR images only with public agencies, and it requires such sharing to be consistent with respect for individuals' privacy. Three of the reviewed agencies share their ALPR images widely using features in the ALPR systems that enable convenient sharing of images with minimal effort. Fresno and Marin have each arranged to share their ALPR images with hundreds of entities and Sacramento with over a thousand entities across the United States. However, we did not find evidence that the agencies had always determined whether an entity receiving shared images had a right and a need to access the images or even that the entity was a public agency. We are concerned that unless an agency conducts verifying research, it will not know who is actually using the ALPR images and for what purpose.

In addition, the agencies have not based their decisions regarding how long to retain their ALPR images on the documented usefulness of those images to investigators, and they may be retaining the images longer than necessary, increasing the risk to individuals' privacy. Fresno's policy is to retain ALPR images for

one year; Sacramento's and Marin's policies specify two years. Los Angeles does not have an ALPR policy, and the lieutenant who administers the ALPR program stated that its protocol is to retain the images for at least five years. However, when we reviewed the agencies' ALPR searches over a six-month period in 2019, we found that personnel for three of the four agencies typically searched for images zero to six months old. Nonetheless, the agencies keep the images far longer.

The agencies we reviewed have few safeguards for the creation of ALPR user accounts and have also failed to audit the use of their ALPR systems. Instead of ensuring that only authorized users access ALPR data for appropriate purposes, the agencies have left their systems open to abuse by neglecting to institute sufficient oversight. Over the years, the media has reported that some individuals within law enforcement used or could use data systems—and sometimes ALPR systems—to obtain information about individuals for their personal use, including to locate places they regularly visit, to determine their acquaintances, and to blackmail them based on this information. ALPR systems should be accessible only to employees who need the data, and accounts should be promptly disabled otherwise. However, the agencies often neglected to limit ALPR system access and have allowed accounts that should be disabled to remain active longer than is prudent. To further ensure that individuals with access do not misuse the ALPR systems, the agencies should be auditing the license plate searches that users perform, along with conducting other monitoring activities. Instead, the agencies have conducted little to no auditing and monitoring and thus have no assurance that misuse has not occurred.

Recommendations

Legislature

To better protect individuals' privacy and to help ensure that local law enforcement agencies structure their ALPR programs in a manner that supports accountability for proper database use, the Legislature should amend state law to do the following:

- Require Justice to draft and make available on its website a policy template that local law enforcement agencies can use as a model for their ALPR policies.

- Require Justice to develop and issue guidance to help local law enforcement agencies identify and evaluate the types of data they are currently storing in their ALPR systems. The guidance should include the necessary security requirements agencies should follow to protect the data in their ALPR systems.
- Establish a maximum data retention period for ALPR images.
- Specify how frequently ALPR system use must be audited and that the audits must include assessing user searches.

Law Enforcement Agencies

To address the shortcomings this audit identified, Fresno, Los Angeles, Marin, and Sacramento should do the following:

- Improve their ALPR policies.
- Implement needed ALPR data security.
- Update vendor contracts with necessary data safeguards.
- Ensure that sharing of ALPR images is done appropriately.
- Evaluate and reestablish data retention periods.
- Develop and implement procedures for granting and managing user accounts.
- Develop and implement ALPR system oversight.

Agency Comments

The four law enforcement agencies we reviewed responded to the draft audit report. Fresno responded that it will use the audit to work to achieve its goal of building trust in its community. Los Angeles responded that it respects individuals' privacy and believes it has policies in place to safeguard information. Nonetheless, it is working on an ALPR policy as required by state law and will perform periodic audits of users' searches. Marin stated it is committed to improvement and will consider the recommendations we made, although it disagreed with several of them. Sacramento stated that it had already begun implementing many of the recommendations, but that it did not agree with how we characterized some of the findings. Justice and the Sacramento County Department of Human Assistance also responded by acknowledging the draft report, although we did not have recommendations directed to either entity.

Blank page inserted for reproduction purposes only.

Introduction

Background

An automated license plate reader (ALPR) is a camera that captures color images of license plates within its field of view. Fixed cameras are mounted on stationary objects, such as light poles, while mobile cameras are mounted on moving objects, such as patrol cars. Software extracts the license plate numbers from the images and stores the images, plate numbers, and dates, times, and locations of the image captures in a searchable database. An *ALPR* system consists of the cameras, the software that reads and converts images of license plates into data, and the searchable database that stores the data. Although the primary focus of each image is the license plate, the image may also show part of the vehicle itself, including individuals within the vehicle, depending on the camera's position. ALPR technology has existed since the 1970s, yet widespread adoption by U.S. law enforcement agencies began only in the mid-2000s. Law enforcement agencies generally view ALPR technology as a valuable tool in achieving their missions.

We conducted a statewide survey of 391 police and sheriff departments, and the survey confirmed that ALPR use is widespread in California: 230 police and sheriff departments currently use an ALPR system, and 36 plan to use one. Table 1 provides an overview of the ALPR systems of the four law enforcement agencies we reviewed as part of this audit.

Table 1
ALPR Systems of Four Audited Law Enforcement Agencies

		NUMBER OF CAMERA SYSTEMS			
LAW ENFORCEMENT AGENCY	NUMBER OF AGENCY PERSONNEL WITH ACCESS TO ALPR DATA	FIXED	MOBILE	CURRENT ALPR VENDOR	DATE AGENCY BEGAN USING CURRENT ALPR VENDOR
Fresno	231	0	8	Vigilant Solutions, LLC	2016
Los Angeles	13,000	3	393	PIPS Technology*	2007
Marin	38	0	3	Vigilant Solutions, LLC	2010
Sacramento	539	33	27	Vigilant Solutions, LLC	2012

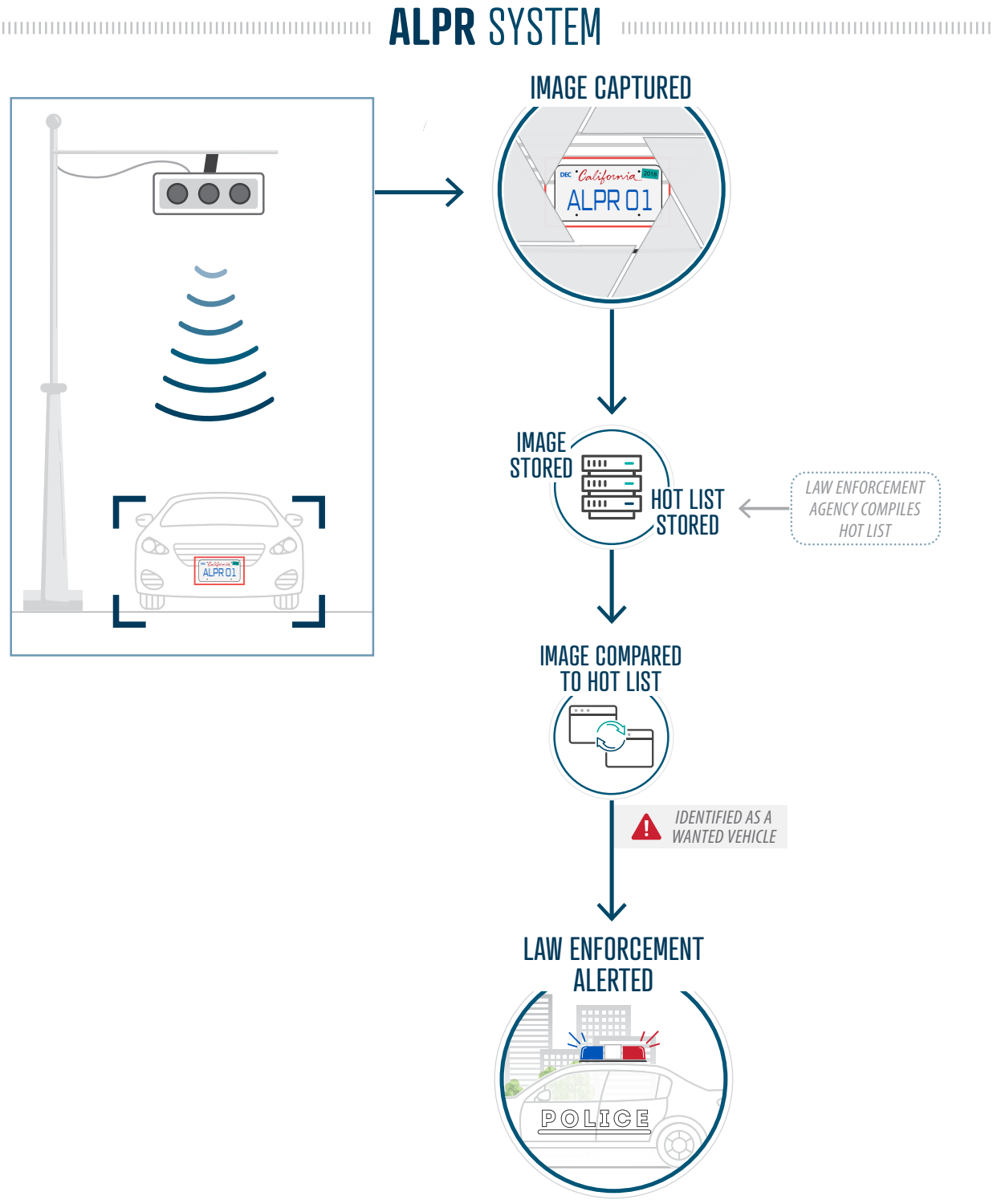
Source: Analysis of reports on ALPR systems as of 2019 and the agencies' survey responses.

* Los Angeles uses PIPS Technology cameras and a user interface from Palantir Technologies, Inc.

An ALPR system is both a real-time tool for law enforcement agencies and an archive of historical information. After the ALPR system identifies a license plate number in an image, it compares the plate number to stored lists of license plate numbers from vehicles of interest, called *hot lists*. Figure 1 shows how an ALPR system uses hot lists to search stored images. Local law enforcement agencies create their own hot lists and also obtain hot lists from state and federal agencies. For example, the California Department of Justice (Justice) provides hot lists to local agencies that include license plate numbers associated with missing persons, gang members, and suspected terrorists. We use the term *ALPR data* to describe all the information stored in an ALPR system, including license plate images and hot lists. Regardless of whether a license plate number matches a plate on a hot list (a *hit*), an ALPR system stores the plate image in a database, creating a searchable archive. Officers may search the database in various ways. For example, they may search for a full license plate number to locate a specific vehicle, search for a partial license plate number to locate a group of vehicles, or search for all vehicles recorded at a particular location at specific times.

Law enforcement agencies can share ALPR data with other public agencies. In the ALPR systems we observed, the agency could choose to share ALPR images only, to share hot lists only, or to share both. Accessing ALPR images shared from other jurisdictions enables agencies to search a broader area, such as across county and state lines. In addition, even if an agency does not operate ALPR cameras itself, it can, through sharing agreements, access ALPR images other agencies collect. Our statewide survey showed that among agencies that operate ALPR systems, roughly 84 percent share their images. Sharing hot lists also enables broader search coverage. For example, an agency could share a hot list that provides license plates linked to wanted individuals with other entities in the region. These entities would then receive hit alerts if their cameras detected those plates.

Figure 1
How ALPR Systems Work



Source: Analysis of David J. Roberts and Meghann Casanova, *Automated License Plate Recognition Systems: Policy and Operational Guidance for Law Enforcement*, International Association of Chiefs of Police, Washington, D.C., 2012.

ALPR Vendors Most Commonly Used in California

Law enforcement agencies typically contract with a third-party vendor for an ALPR system. In our statewide survey, most—70 percent—of those that have an ALPR system reported using a company called Vigilant Solutions, LLC (Vigilant). Figure A.1 in Appendix A summarizes these responses. Three of the agencies we reviewed—the Fresno Police Department (Fresno), Marin County Sheriff's Office (Marin), and Sacramento County Sheriff's Office (Sacramento)—contract with Vigilant. The Vigilant ALPR system provides a user interface to search license plates and the option to share ALPR images and hot lists with other agencies through the Vigilant system. Fresno, Marin, and Sacramento all store their ALPR images on Vigilant's server, which is a cloud service, and share their images with other agencies that subscribe to Vigilant's services. Roughly 22 percent of the survey respondents that have ALPR systems use a company called PIPS Technology. One of the agencies we audited in depth, the Los Angeles Police Department (Los Angeles), purchased its cameras from PIPS Technology, but it stores the images on its own server. Los Angeles uses a software platform called Palantir for the user interface that allows for searches of its ALPR images, and it shares its ALPR images with other agencies in the region that use the Palantir user interface.

Key Elements Law Enforcement Agencies Must Include in Their ALPR Usage and Privacy Policy

- The authorized purpose for using the ALPR system and collecting, accessing, or using ALPR data.
- 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 data.
- The training requirements for those employees and independent contractors authorized to use or access the ALPR system, or to collect ALPR data.
- A description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws.
- The purposes of, process for, and restrictions on the sale, sharing, or transfer of ALPR data.
- The length of time ALPR data will be retained, and the process for determining if and when to destroy retained ALPR data.

Source: Analysis of state law.

State Laws Governing ALPR Systems and Data Sharing

With few exceptions, California law requires public agencies that operate and use ALPR systems to implement a usage and privacy policy. The Legislature passed Senate Bill 34 (Statutes of 2015, Chapter 532) (SB 34), effective January 1, 2016, to establish requirements regarding the operation and use of ALPR systems. This law generally requires public agencies, including law enforcement agencies, that operate or use an ALPR system to maintain reasonable security procedures and practices to protect ALPR data, to implement a usage and privacy policy, to make that policy available to the public, and to post that policy on its website should the agency have one, among other provisions. The text box describes required elements of an agency's ALPR usage and privacy policy.

SB 34 does not specify retention periods for ALPR data, although another state law limits the California Highway Patrol (CHP) to retaining its ALPR images for no more than 60 days, unless those images are being used for felony investigations or as evidence. Agencies implementing ALPR programs after January 1, 2016, must also provide an opportunity for public comment before implementing the program.

In 2018 another state law took effect that limits the information law enforcement agencies can share for immigration enforcement purposes and requires Justice to issue guidance to state and local law enforcement agencies regarding these limitations as they apply to law enforcement databases. In October 2018 Justice issued this guidance, which can also serve as best practices for law enforcement agencies on how to lawfully share ALPR images. The guidance encourages law enforcement agencies that maintain databases to inquire about the purpose for which the other law enforcement agency intends to use the information contained in the database. If a law enforcement agency intends to use the information for immigration enforcement purposes, Justice states that law enforcement agencies should require, as a condition of accessing the database, an agreement that stipulates that access will be made only in cases involving individuals with criminal histories, or for information regarding the immigration or citizenship status of an individual. Beyond this guidance and the hot lists Justice provides to local law enforcement agencies, as we describe earlier, Justice plays no other role in ALPR programs.

State law requires law enforcement agencies to maintain reasonable security procedures and practices to protect ALPR data from unauthorized access, destruction, use, modification, or disclosure. These requirements mean that ALPR data are sensitive. For comparison purposes, the California Department of Technology Office of Information Security defines *sensitive data* for state agencies as information that requires special precautions to protect it from unauthorized use, access, disclosure, modification, loss, or deletion. In addition to ALPR images and hot lists, a law enforcement agency can enter other information into its ALPR system, such as personal information and criminal justice information. *Personal information* is information that identifies or describes an individual, including name or physical description. SB 34—whose purpose was, in part, to institute reasonable privacy standards for the operation of ALPR systems—requires that ALPR data be protected with reasonable operational, administrative, technical, and physical safeguards to ensure their confidentiality. Thus, personal information in an ALPR system also requires appropriate and reasonable safeguards. *Criminal justice information*, as defined by the Criminal Justice Information Services Division (CJIS) of the U.S. Federal Bureau of Investigation (FBI), refers to data necessary

for law enforcement and civil agencies to perform their missions. This includes information about vehicles associated with crimes, when accompanied by personal information.

When CJIS provides criminal justice information to law enforcement agencies, it requires those agencies to comply with a minimum set of information technology (IT) security requirements to protect the information, and these requirements can serve as best practices for agencies to follow. Because an agency can enter personal information and criminal justice information into its ALPR system, either as part of a hot list or as a comment added as part of a license plate search, all ALPR data are sensitive and require appropriate safeguards.

Privacy Concerns Related to ALPR Systems

Although law enforcement agencies collect ALPR images in public view, and there is no reasonable expectation of privacy regarding a license plate, the use and retention of those images raises privacy concerns. The agencies we reviewed accumulate a large number of images in their ALPR systems. For example, Sacramento recorded 1.7 million images in one week, and Los Angeles currently has more than 320 million images in its ALPR database that it has accumulated over several years. The majority of these images do not generate hit alerts. For example, data from the Los Angeles system show that at the time of our review only 400,000 (0.1 percent) of the 320 million images Los Angeles has stored generated an immediate match against its hot lists for vehicles associated with car thefts, felonies, or warrants. However, the stored images provide value beyond immediate hit alerts, as law enforcement personnel can search the accumulated images to target the whereabouts of vehicles at particular times or locations. This storage, retention, and searching of the images, although valuable to law enforcement, has the potential to infringe on individuals' privacy.

Organizations such as the American Civil Liberties Union (ACLU) have criticized law enforcement agencies' collection of ALPR images because of the risks it poses to privacy. The ACLU stated that increasing numbers of cameras, long data retention periods, and sharing of ALPR images among law enforcement agencies allow agencies to track individuals' movements in detail, and it has voiced concerns that such constant monitoring can inhibit the exercise of free speech and association. The ACLU has also raised concerns that law enforcement officers could inappropriately monitor the movements of individuals such as ex-spouses, neighbors, and other associates. There have been occurrences of officers misusing law enforcement databases like those that contain ALPR images. In 2016 the Associated Press conducted a review that found more than

325 instances between 2013 and 2015 in which law enforcement officers who misused databases were fired, suspended, or resigned, and more than 250 instances of reprimands or lesser discipline related to such misuse. For example, the Associated Press reported on a police sergeant in Ohio who pleaded guilty to stalking his ex-girlfriend after he searched law enforcement databases for personal information about her and also the woman's mother, her close male friends, and students from a course she taught.

Law enforcement has recognized the privacy concerns posed by the operation of ALPR systems, yet it has also pointed to the usefulness of the systems. For example, the Police Executive Research Forum (police research forum) and the Mesa Police Department (Mesa) in Arizona conducted a study of the effectiveness of ALPR systems for Mesa's auto theft unit in 2011. They found that officers got nearly three times as many stolen vehicle hits and made about twice as many vehicle recoveries when using an ALPR system, compared to officers performing manual license plate checks. Law enforcement has also found ALPR systems useful for investigations. For example, the assistant chief of the Minneapolis Police Department told the police research forum in 2012 that the department located a vehicle associated with a domestic kidnapping case by searching ALPR images. With regard to the retention of ALPR images, the International Association of Chiefs of Police (chiefs' association) acknowledged the tension between long retention periods and privacy. The chiefs' association noted that a reluctance to destroy records may stem from investigators' experience that seemingly irrelevant or untimely information may acquire new significance as an investigation brings further details to light. However, the chiefs' association also recognized the privacy risks of ALPR images. In a 2009 report, it stated that mobile ALPR cameras could record license plate numbers of vehicles parked at addiction counseling meetings, doctors' offices, and staging areas for political protests. The chiefs' association argued that establishing policies regulating ALPR programs could mitigate privacy concerns, and it produced a report in 2012 offering guidance on developing such policies.

Federal Guidance on Privacy Protection

As far back as 1973, the federal government acknowledged that individuals' privacy needs to be protected from arbitrary and abusive record-keeping practices. The U.S. Department of Health, Education, and Welfare, as it was then known, identified principles for the fair collection, use, storage, and dissemination of personal information by electronic information systems. Over time the principles were adapted into information practices. According to the U.S. Government Accountability Office, a revised version of the information practices was published in 1980 by

the Organization for Economic Cooperation and Development (OECD)—an international organization that works with governments, policymakers, and citizens on social, economic, and environmental challenges—and with some variation, these practices form the basis of privacy laws in the United States and around the world. The OECD updated its eight information practices in 2013, and California's lawmakers included many of these information practices in SB 34. For example, the OECD's information practices describe the importance of an organization specifying the purposes for which it is collecting and using data; keeping data reasonably safe from the risk of unauthorized access, destruction, use, modification, and disclosure; being open about policies involving data; and being accountable for complying with the information practices.

The U.S. Supreme Court (court) has not directly decided a case that we could find addressing ALPR images, although it has decided cases involving other electronic surveillance. Because license plates are in plain view, the collection of license plate images by law enforcement is not a per se violation of the Fourth Amendment's prohibition against unreasonable searches and seizures. However, the court has found that certain electronic data that reveal individuals' movements over an extended period of time, if gathered, do at some point impinge on privacy. The court has specifically addressed these issues with respect to the use of global positioning system (GPS) data and cell-site location information, which is location information linked to cellphone use. Cell-site location information—similar to ALPR images—provides data on an individual's continuous movements over a potentially unlimited period of time. In a 2018 case involving cell-site location information, the court stated that "[a] person does not surrender all [privacy] protections by venturing into the public sphere." The court continued, "With access to [cell-site location information], the Government can now travel back in time to retrace a person's whereabouts," and noted that the information was collected on everyone, not only "persons who might happen to come under investigation." Thus, even though case law on electronic data that enable tracking of individuals' movements over an extended period of time is still evolving, the court has recognized that privacy implications exist for such data, which can include ALPR images.

Audit Results

The Four Law Enforcement Agencies We Reviewed Have Not Consistently Fulfilled Requirements Designed to Protect Individuals' Privacy

California's lawmakers drafted current ALPR law to institute reasonable privacy standards for the operation of ALPR systems. As we discuss in the Introduction, technology gives governments the ability to accumulate significant amounts of information about people, raising the question of how individuals' privacy is to be preserved, and the federal and state governments and courts have issued laws and guidance—including, in the case of California, SB 34—related to the use of such information.

Yet local law enforcement agencies—specifically the four agencies we reviewed—have not done all they could to respect individuals' privacy by incorporating the requirements and concepts in SB 34 into their operations. With few exceptions, SB 34 requires a public agency that operates or uses an ALPR system to implement a usage and privacy policy that describes how the system will be used and monitored to ensure the security of the ALPR data accessed or used. The agencies we reviewed have mature ALPR programs—they have been using their current ALPR vendors since as far back as 2007. However, as we discuss later, we found that the agencies have risked individuals' privacy by not making informed decisions about sharing ALPR images with other entities, by not considering how they are using ALPR data when determining how long to keep it, by following poor practices for granting their staff access to the ALPR systems, and by failing to audit system use.

State law requires law enforcement agencies to administer ALPR programs in ways that respect individual's privacy and protect ALPR data. The law also requires the agencies to have a written usage and privacy policy that sets forth how they will operate and use their ALPR systems. These usage and privacy policies must include the following elements:

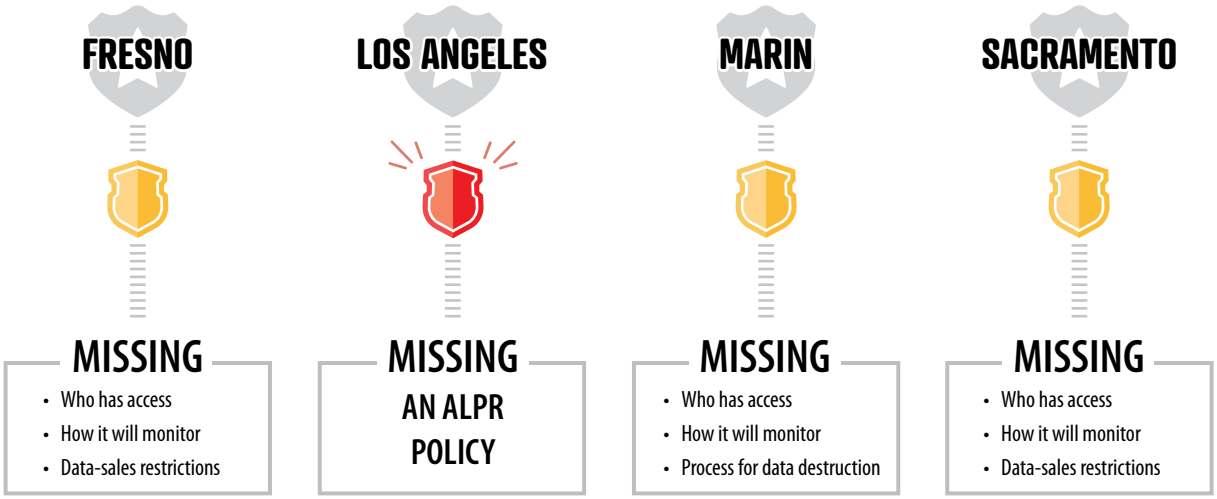
- Authorized purposes for using the ALPR system and collecting the data.
- A description of the job title or other designation of individuals who are authorized to use or access the ALPR system.
- Training requirements for the authorized individuals who will use or access the ALPR system.
- A description of how the agency will monitor the ALPR system to ensure the security of the data and compliance with privacy laws.

- The purpose of, process for, and restrictions on the sale, sharing, or transfer of ALPR data.
- The length of time the ALPR data will be retained and the process used to determine if and when to destroy retained ALPR data.

Agencies may expand on these required elements as needed to ensure that their collection, use, maintenance, sharing, and dissemination of ALPR data are consistent with respect for individuals' privacy.

None of the four agencies we reviewed have an ALPR policy that contains all of the required information, thereby contributing to the agencies' failure to implement programs that reflect the privacy principles in SB 34. Los Angeles has not developed an ALPR policy, and the policies of the other three agencies are deficient in various ways, as Figure 2 shows. For example, all have failed to fully address how they will monitor system use to ensure compliance with applicable privacy laws, which likely contributed to their failure to institute regular audits of user searches. The agencies could have avoided concerns such as those shown in Figure 2, which we describe later in this report if they had developed more thorough policies. Clear policies that define the purposes and procedures for monitoring ALPR systems help agencies meet their goals.

Figure 2
The Agencies' ALPR Policies Are Missing Required Key Elements for Respecting Individuals' Privacy



Source: State law and the agencies' ALPR policies as well as interviews with the agencies' management.

As a result of our audit, each of the four agencies is making or considering changes to its policies. The ALPR administrators at Fresno, Marin, and Sacramento agreed that their policies did not contain one or more elements required by state law. They also explained that they did not include certain policy requirements they believed did not apply to their use of ALPR data. For example, Sacramento's ALPR policy does not describe ALPR data-selling restrictions because, according to the ALPR administrator, Sacramento does not currently sell ALPR data. However, because their policies are incomplete and do not specify what personnel cannot do when interacting with their ALPR systems, these three agencies left out critical guidance to staff and increased the risk that staff would use the ALPR system inappropriately. The program administrators at Fresno, Marin, and Sacramento told us that they will consider changes to their policies subsequent to our audit. Although the lieutenant who serves as Los Angeles' program administrator initially believed that the agency's many IT policies covered the ALPR program, when we brought the deficiencies in oversight to his attention, he acknowledged the need for Los Angeles to have an ALPR policy and began drafting one in October 2019.

Fresno, Marin, and Sacramento have incomplete ALPR policies, which increases the risk that staff will use the ALPR systems inappropriately.

We are concerned that the policy deficiencies we found are not limited to the agencies we reviewed, and thus law enforcement agencies of all types may benefit from guidance to improve their policies. We surveyed 391 police and sheriff departments statewide about their ALPR programs, and many stated that they have ALPR policies and that these policies are publicly available. Because state law requires each agency that operates or uses an ALPR system to implement a usage and privacy policy, and to make the policy available to the public in writing and post it conspicuously on the agency's website, we inquired about how agencies throughout the State were adhering to these requirements. Of the law enforcement agencies using an ALPR system, 96 percent responded that they have ALPR policies. Of this group, at least 70 percent stated that they have posted their policy to their website. A breakdown of the law enforcement agencies' responses to our survey can be found at http://auditor.ca.gov/reports/2019-118/supplemental.html. However, we believe it is likely that many of the survey respondents will have the same problems with the quality and completeness of their policies as the four agencies we visited. As we discuss in the Introduction, Justice has issued guidance to law enforcement agencies to help them understand how to adhere to state law regarding the sharing of information for immigration enforcement purposes. Given Justice's experience and broad reach in the law enforcement community, developing guidance for local law enforcement agencies on needed policy elements could improve the quality and completeness of their policies.

The Law Enforcement Agencies Have Often Placed Their ALPR Data at Risk

Administering ALPR programs in ways that respect individuals' privacy requires a thoughtful and considered approach to data management that the agencies we reviewed have not always taken. Specifically, three of the agencies have agreed to share their images widely with little knowledge of the receiving entities and their need for the images. Moreover, the agencies have not based their decisions regarding retention of images on their actual usefulness to investigators and may be retaining the images longer than necessary, increasing the risk to individuals' privacy.

The Agencies May Not Be Adequately Protecting Their Sensitive ALPR Data

Law enforcement users can upload personal information and criminal justice information into the Vigilant system through hot lists and open text fields.

Law enforcement agency personnel can upload or enter sensitive information into their ALPR systems, which may require specific safeguards. As we discuss in the Introduction, this sensitive information could include personal information and criminal justice information. In addition, these data may originate from the California Law Enforcement Telecommunications System (CLETS)—a system that allows law enforcement agencies to obtain information from federal and state databases, such as arrests and fingerprint records from Justice. In reviewing multiple agencies' ALPR policies, we found several that stated that their ALPR systems may contain information obtained through CLETS. Additionally, in a security and compliance memorandum, Vigilant acknowledged that law enforcement users can upload personal information and criminal justice information into the Vigilant system through hot lists and open text fields.

For example, in addition to license plate images, Sacramento and Los Angeles add data to their systems such as criminal charges and warrant information, in combination with personal information such as names, addresses, dates of birth, and physical descriptions. The added data can be in the form of hot lists that agencies use to search for license plates of interest, as shown in Figure 1 in the Introduction, or they can be data that are entered into open text fields. By running an automated function each day, Sacramento extracts information from several databases and uploads the information as hot lists to its ALPR system. Los Angeles does not create its own hot lists, but it regularly downloads hot lists from Justice and the Los Angeles County Sheriff's Department, then uploads the hot lists to its ALPR system. Another way that information in addition to license plate images gets into an ALPR system is by users adding it to open text fields. Data entered into open text fields are generally associated with license plate searches.

When conducting a search, staff are prompted to enter a case number and the purpose of the search, and they may do so by typing in text. The ALPR systems store this open text in their audit logs, which detail user activity and the reasons for the activity.

In contrast to Sacramento and Los Angeles, Marin and Fresno occasionally upload hot lists into their ALPR systems. With regard to open text fields, we reviewed the audit logs for Marin and Fresno and did not find personal information in combination with other sensitive information in the six months of search records we studied. However, the possibility exists that law enforcement personnel could enter sensitive information into open text fields during ALPR searches.

When an IT system lacks sufficient security, the system is at risk of misuse and data breaches.

When an IT system lacks sufficient security, the system is at risk of misuse and data breaches. Systems containing personal information and criminal justice information must have adequate protections to assure individuals' privacy. However, as discussed in the Introduction, ALPR data can originate from different sources, and the source of the information may drive some of the required IT security protocols. On one hand, CJIS developed a policy that dictates the minimum standards that law enforcement agencies must follow to protect criminal justice information they obtain from the FBI (CJIS policy). On the other hand, users of Justice's CLETS system must follow the protections outlined in the CLETS *Policies, Practices and Procedures* document, which describes formal security measures law enforcement agencies must follow to access and protect CLETS information in addition to the CJIS policy requirements.

Further, it can be difficult to know what protections to apply to data from different sources. For example, an individual's address obtained by searching the Department of Motor Vehicles database through CLETS would be subject to Justice's data security requirements, but the same information obtained from a local law enforcement agency database would not. Moreover, the personal information Los Angeles and Sacramento have entered into their ALPR search records does not include its origin, making the required level of protection unclear.

Given these issues and the need to identify a standard that can be uniformly applied to ALPR data regardless of their source, we believe that CJIS policy provides reasonable security measures for law enforcement agencies to protect all of their ALPR data. State law requires these agencies to maintain reasonable security procedures and practices to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure. CJIS policy specifies operational, administrative, technical, and physical safeguards for each of these areas. For example, CJIS policy

requires agencies to ensure that their sensitive data are encrypted, and it limits physical access to specific personnel authorized to access the data. Nearly all of the 230 agencies that reported using ALPR systems in response to our statewide survey—including Fresno, Los Angeles, Marin, and Sacramento—reported that their ALPR data storage solution complies with CJIS policy.

We are concerned that the agencies using Vigilant may not be protecting their ALPR data in conformity with CJIS policy standards.

Nevertheless, we are concerned that the agencies using Vigilant may not be protecting their ALPR data in conformity with CJIS policy standards. Fresno, Marin, and Sacramento store their ALPR data in Vigilant's cloud database, and CJIS policy requires agencies to ensure that the cloud vendors that store and process their criminal justice information comply with its security requirements. Such requirements include controlling physical access to sensitive data, encrypting the data, and conducting background checks and training for employees with access to criminal justice information. In addition, before providing sensitive data to a vendor, CJIS requires law enforcement agencies to identify necessary authentication and monitoring controls, such as two-factor authentication and activity logging. Because the Vigilant software is by default accessible via the Internet, an officer may be able to access it using his or her personal device. The ability to access ALPR data in this manner bypasses the agencies' network security safeguards and violates CJIS policy requiring agencies to monitor and control access to the data.

One way to prevent users from signing in to the Vigilant system using personal devices would be to implement authentication controls, such as two-factor authentication. Two-factor authentication involves a second level of verification, such as a passcode sent to a specific device, and allows agencies to require that the passcode be sent only to department-issued devices. Although Vigilant offers two-factor authentication, Marin, Fresno, and Sacramento do not use it. CJIS policy requires two-factor authentication only for systems that directly access federal systems. However, this requirement recognizes that two-factor authentication is more secure than a basic username and password login for systems like Vigilant that are accessible over the Internet. Thus, two-factor authentication could serve as a best practice for agencies to prevent inappropriate access to their ALPR systems.

In addition, monitoring the activity logs can alert program administrators to unauthorized access of their ALPR systems. CJIS policy requires agencies to monitor access to systems that contain criminal justice information. Vigilant provides its clients with logs of network addresses that have accessed their ALPR systems, and although Marin's ALPR program administrator stated that he reviews these logs, administrators from Sacramento and Fresno confirmed that they do not. Reviewing the logs of system access

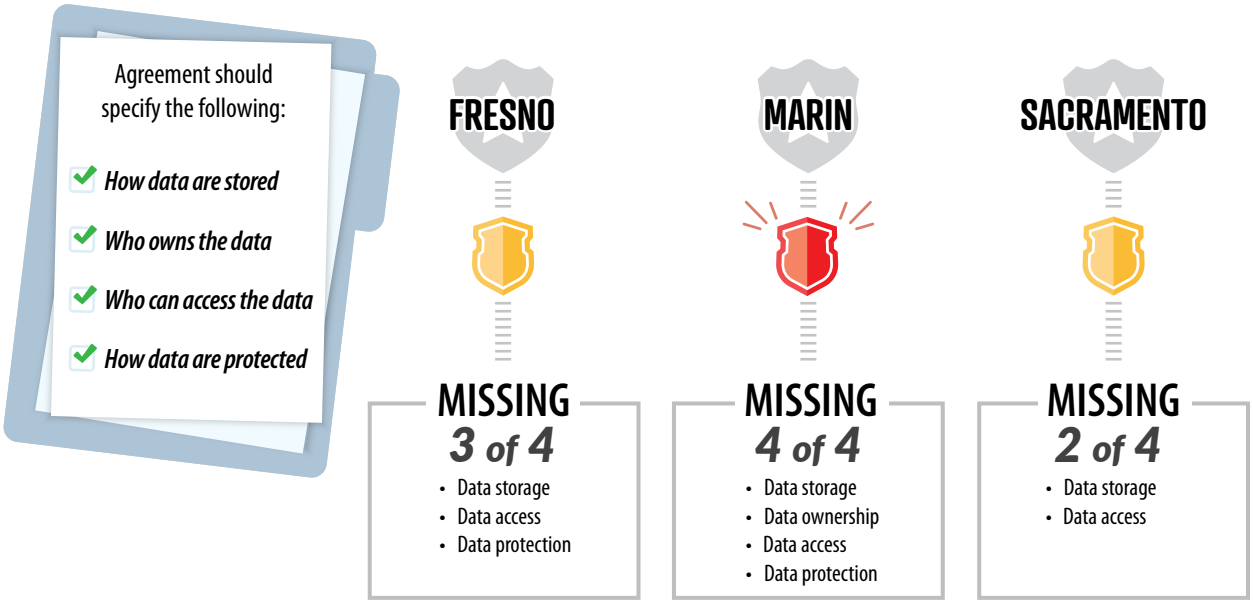
could help the agencies monitor access to their ALPR systems and detect whether someone accesses the ALPR system from an unrecognized network address.

When law enforcement agencies provide sensitive information to ALPR vendors, their contracts should provide assurance that the vendor will adequately protect that information. CJIS policy recommends several provisions that law enforcement agencies should consider including in their contracts to ensure that cloud vendors adequately protect criminal justice information. For example, a contract that protects a law enforcement agency's data would make clear that the agency owns the data it uploads into the ALPR system, that the agency's data will not be stored outside of the United States or Canada, and that employees at the cloud vendor who have access to unencrypted criminal justice information will undergo training and background checks. Without these contract provisions, agencies lack guarantees that the cloud vendor will implement appropriate protections of their data.

We found that the three agencies storing ALPR data in Vigilant's cloud—Fresno, Marin, and Sacramento—do not have sufficient data security safeguards in their contracts.

We found that the three agencies storing ALPR data in Vigilant's cloud—Fresno, Marin, and Sacramento—do not have sufficient data security safeguards in their contracts. As Figure 3 shows, none of the agencies' contracts with Vigilant meet all of the CJIS data security requirements. For example, the agencies' contracts do not state that Vigilant will store their data in the United States or Canada. Marin's contract does not make clear that Marin owns the data it adds to the ALPR system. It is important to note that Vigilant claims to implement data security measures that comply with CJIS policy. In a security and compliance memorandum, Vigilant lists steps it takes to encrypt data that may contain criminal justice information, as well as physical and network security safeguards it has in place to prevent unauthorized access to its ALPR cloud. We have no basis to dispute Vigilant's claims, but without strong contract provisions requiring CJIS safeguards, the three agencies have no guarantee that Vigilant will protect their data. As CJIS policy states, ambiguous contract terms can lead to controversy over data privacy and ownership rights, whereas a contract that clearly establishes data ownership acts as a foundation for trust that the cloud vendor will protect the privacy of the agency's data.

Figure 3
The Agencies' Existing Agreements With Vigilant Do Not Contain Adequate Data Security Measures



Source: Agencies' agreements with Vigilant and CJIS policy requirements.

A lack of IT department involvement and outdated contracts likely contributed to the data security weaknesses we observed. Fresno, Marin, and Sacramento have IT units that administer their systems and ensure compliance with Justice's data security requirements. However, at Fresno and Marin, the IT units are responsible for network security and have little oversight of the ALPR systems' data security. According to Fresno's IT manager, Fresno's main IT unit does not manage user accounts or monitor access to the ALPR system. Fresno has an IT analyst separate from the main IT unit who currently helps administer user accounts and provides technical support for the ALPR system; however, his background is not in network security. A deputy in Marin's auto theft unit manages Marin's entire ALPR system—including user accounts and training. This arrangement is not ideal, since individuals outside of an agency's IT department may lack the expertise necessary to implement adequate data security safeguards. According to Sacramento's ALPR administrator, Sacramento's IT unit recently assumed responsibility for the ALPR system, but before about April 2019, an officer outside of the IT unit administered the ALPR system.

In addition, with the exception of Sacramento, the agencies have not updated their contract terms with Vigilant for several years. The agencies' contracts renew each year when the agencies pay a service fee to Vigilant. As a result, Fresno has not updated its contract for three years, and Marin for nine years. Sacramento updated

its contract terms with Vigilant in September 2019, after using its previous agreement for seven years. Agreements that are not kept current may reflect outdated practices or omit needed assurances, increasing the risk that data are not protected.

Los Angeles was not able to demonstrate that it has an agreement in place to protect its ALPR data from inappropriate access.

Los Angeles was not able to demonstrate that it has an agreement in place to protect its ALPR data from inappropriate access. Los Angeles stores its ALPR data in a city-controlled data center rather than in a vendor cloud like the agencies that use Vigilant. Nevertheless, Los Angeles contracts with Palantir for IT support, and the FBI's 2017 audit of Los Angeles' data security practices identified Palantir as an entity with access to criminal justice information; thus we expected Los Angeles' agreement with Palantir to meet CJIS policy requirements. CJIS policy requires agencies to enter into agreements with vendors that access their criminal justice information. The agreements are to include an FBI-drafted security addendum that outlines specific safeguards a vendor agrees to put in place to comply with CJIS policy and an acknowledgment by the vendor of the great harm that may arise from misusing sensitive data. However, in response to our request for its agreement with Palantir, Los Angeles produced two expired contracts and a 2018 commodities agreement extending its licensing and support for Palantir software. None of these documents contained the FBI-drafted security addendum. Thus Los Angeles was not able to demonstrate that its agreement with Palantir contains appropriate data protections to ensure that Palantir employees with access to Los Angeles' ALPR data will not use the data for unauthorized purposes.

The Agencies Have Not Made Informed ALPR Image-Sharing Decisions

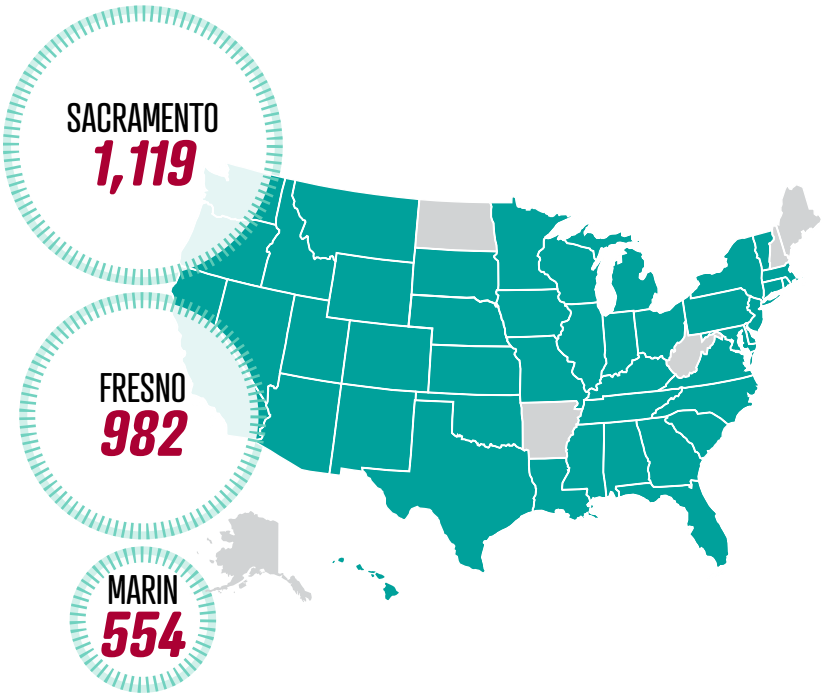
A significant feature of ALPR systems is their ability to share information with users across other organizations. A variety of requirements and guidance exist regarding how law enforcement agencies should share ALPR data, including images. ALPR images contain the date, time, and location of the scanned license plate and largely relate to vehicles that are not linked to crimes. The risk that the images will be misused rises as the images are more widely distributed, and there are numerous examples of law enforcement officers misusing their access to various databases. For example, an Associated Press article from 2016 reported a case from the state of Georgia in which an officer accepted a bribe to search for a woman's license plate number to see whether she was an undercover officer. Although such an example of misconduct is not representative of all law enforcement personnel, it illustrates the need for appropriate safeguards over law enforcement tools. Once a license plate is tied to an individual's identity, which is easy for a law enforcement officer to do, ALPR images may make it possible to track that individual's movements.

State law allows local law enforcement agencies to share ALPR images only with public agencies and requires sharing to be consistent with respect for individuals' privacy. Further, guidance that Justice issued in October 2018 addresses the agencies' governance of databases in relation to immigration enforcement, and this guidance provides a best practice for sharing in general. In the guidance, Justice encourages law enforcement agencies to inquire regarding the purpose for which an agency seeking access to their database intends to use the information and then, as a condition for accessing the database, to require agreements ensuring appropriate use of the data if its purpose includes immigration enforcement. The chiefs' association also recommends that law enforcement agencies maintain ALPR image-sharing records that include information on how the requester intends to use the images. The four agencies we reviewed asserted that they share ALPR images with others on the principle that these entities have a right and need to know the information. Because following state law necessitates establishing an agency's identity, i.e., the right to know, and Justice's guidance suggests establishing the purpose, i.e., the need to know, for which an agency intends to use the images, the agencies' position seems consistent with state law and Justice's guidance.

However, we had difficulty determining whether the reviewed agencies have actually made informed decisions about sharing their ALPR images. Fresno and Marin have each approved sharing their ALPR images with hundreds of entities, and Sacramento with over a thousand. Many of these entities are within California, but they also span most of the other 49 states. Figure 4 shows the entities' locations, illustrating how widely distributed access to these ALPR images is. In addition, we could not always ascertain how the agencies determined whether an entity receiving access to images had a right and need to access them or even whether the entity was a public agency. We reviewed the lists of entities and found one that appeared to be a non-public entity and others that were unidentifiable because they were listed only by initials. For example, Fresno, Marin, and Sacramento all approved an entity listed as the Missouri Police Chiefs Association (Missouri Association); however, this is not a public agency but rather a professional organization that provides training opportunities and advocates for pro-law enforcement legislation. However, none of the agencies could demonstrate that they had evaluated the Missouri Association before sharing images, nor could they tell us why the Missouri Association had a right to those images. When we inquired with Vigilant, an official explained that despite the name, it is the Missouri State Highway Patrol—a law enforcement agency—that uses the account. The lists contain many other entities whose identities and law enforcement purposes are not immediately evident. Unless a law enforcement agency verifies each entity's identity and its right to view the ALPR images, the agency cannot know who is actually using them. Although the three agencies reviewed their sharing arrangements to varying degrees during our audit, none could demonstrate that they perform this kind of verification before sharing their ALPR images.

We could not always ascertain how the agencies determined whether an entity receiving access to images had a right and need to access them or even whether the entity was a public agency.

Figure 4
Three Agencies Have Authorized Sharing With Entities Located in States Across the Nation



Source: Analysis of data-sharing reports from the Vigilant system.

Similarly, even when an entity is a verified public agency, it is not always evident that agencies are making informed decisions by establishing the entity's need for the ALPR images. Fresno, Marin, and Sacramento all authorized sharing with the Honolulu Police Department, but given the distance between California and Hawaii and the limited instances of cars traveling between the two states, it is uncertain whether the Honolulu Police Department has a persuasive need for these ALPR images. Fresno's ALPR administrator agreed that not a great deal of thought went into its decision to share with the Honolulu Police Department, and he believes that it probably authorized the share because the entity was a law enforcement agency. In contrast, Marin's ALPR administrator believes that sharing ALPR images widely is important because the more information available to law enforcement, the more successful it can be in its mission. However, sharing decisions should also consider the importance of protecting individuals' privacy. Each authorized share exposes the ALPR images to greater risk of misuse; therefore, the agencies should approach each sharing request individually based on the requester's actual need for the images.

The three agencies have also relied on features in Vigilant's software rather than establishing their own practices for sharing their ALPR images. A sound approach to sharing would include establishing each requesting entity's need to know and right to know and keeping records of the assessment and resulting decision. However, none of these agencies maintain records outside of the Vigilant user interface of when or why they agreed to share with particular entities, and neither Marin nor Sacramento includes a process for approving sharing requests in their ALPR policies as state law requires. Fresno has outlined procedures that incorporate these elements, but it has not followed them. Fresno's ALPR administrator explained that its procedures require more information than an entity requesting a share provides in the Vigilant user interface, and there has been frequent turnover in the position responsible for approving sharing requests.

Current administrators at the three agencies have difficulty understanding when and how sharing occurred because the information the Vigilant user interface displays has changed over time. The status of a sharing relationship in the Vigilant system depends on whether the involved entities' accounts are *active* or *inactive*. Active entities have a current account with Vigilant while inactive entities do not. An agency may agree to share with an active entity that later becomes inactive. Images cannot be shared between active and inactive entities. However, unless an agency deliberately removes a sharing relationship with an inactive entity, that sharing relationship remains and would become operational if an inactive entity decided to renew its account with Vigilant and become active once more. Previously, Vigilant had structured its user interface so that inactive entities did not appear in the sharing report that shows a list of entities with whom an agency had agreed to share. Recently, Vigilant changed its interface to make inactive entities visible. Whether an entity is active is not apparent from the sharing report alone.

A change in the vendor's user interface and not keeping records of authorized shares made it difficult for ALPR administrators to track current sharing relationships.

This change in the user interface and the fact that agencies kept no records of the shares they have authorized made it difficult for ALPR administrators at the agencies to know the status of current sharing relationships. For example, in 2014 a prior ALPR administrator for Marin had agreed to share images with three U.S. Immigration and Customs Enforcement (ICE) agencies. In December 2018, Marin's current ALPR administrator used the Vigilant user interface to review the sharing report and noted that the report included no ICE agencies. However, when he reviewed the report again in August 2019—at our request—three ICE agencies appeared on the list. We discussed this discrepancy with Vigilant, which explained that the three ICE agencies were currently inactive. When Marin's ALPR administrator reviewed the sharing report in December 2018, inactive agencies did not appear on the report, but Vigilant subsequently changed its user interface so that inactive

agencies did appear. Although the ICE agencies could not access Marin's ALPR images because they were inactive, to effectively end the share, Marin needed to remove the authorization for sharing with the ICE agencies, which Marin has since done.

According to Marin's ALPR administrator, it is now the department's position that it will not share images with ICE, but if it had remained unaware that the sharing relationships existed and the ICE agencies had become active again, it would have been sharing its ALPR images with them without knowing it was doing so. Had Marin kept its own records of the sharing to which it had agreed, it would have been aware that it had agreed to share with ICE in the past, and it would have been able to remove those shares promptly. Sacramento had also authorized sharing to ICE agencies in the past. When the current ALPR administrator reviewed the list of entities with which it shared images with in response to our audit, he removed those shares as well. In contrast, Fresno had never authorized any sharing relationship with an ICE agency.

Although none of the agencies using Vigilant currently share with ICE agencies, all three had authorized shares with entities with border patrol duties. Despite not having implemented any agreements related to this sharing since Justice issued its guidance in October 2018, the three agencies were all sharing with the San Diego Sector Border Patrol of U.S. Customs and Border Protection at the start of our audit. During our audit, Sacramento removed the share to this agency. Marin and Sacramento had also authorized sharing with an agency listed as "California Border Patrol," and although Sacramento removed this share at the same time it removed the shares to ICE, Marin continues to share with this entity. Fresno continues to share with the Customs and Border Protection National Targeting Center. Although Sacramento had also authorized a share to this entity, it removed this share during our audit. All of these entities' duties could potentially intersect with immigration enforcement. Justice's guidelines for sharing data are particularly relevant in these cases, yet the agencies were either unaware of these guidelines or had not implemented them for their ALPR systems.

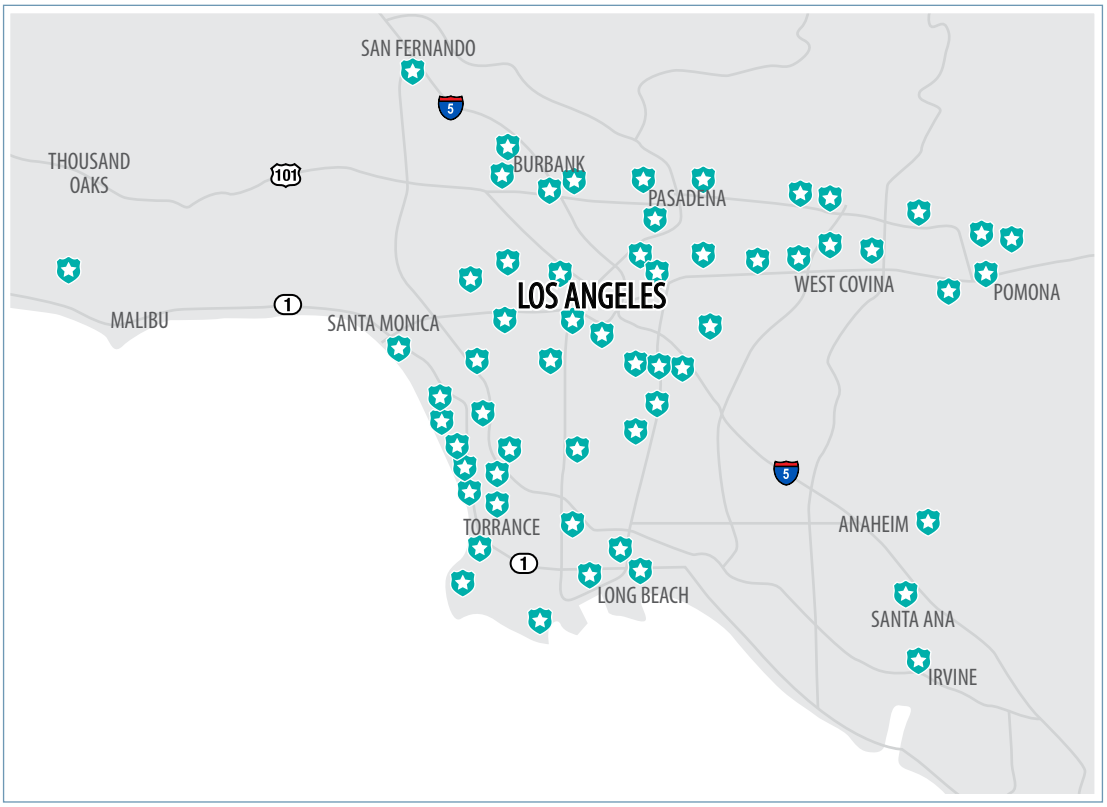
Justice's guidelines for sharing data are particularly relevant, yet Fresno, Marin, and Sacramento were either unaware of these guidelines or had not implemented them for their ALPR systems.

Of the four agencies we reviewed, only Fresno and Sacramento share hot lists they create, and they do so through a more controlled process than for sharing ALPR images. Vigilant's user interface enables hot-list sharing in addition to sharing ALPR images. In contrast to its wide sharing of ALPR images, Fresno shares the hot lists it occasionally uploads with only three law enforcement agencies in the nearby region. Sacramento has agreed to share six hot lists with eight law enforcement agencies in California. With each agency, Sacramento took the additional step of developing a memorandum of understanding providing guidelines for sharing the hot lists and the signature of the chief official at each agency.

Although the memorandum does not specify which hot lists Sacramento will share, it does provide a record of the entities with which hot-list sharing occurred, unlike its sharing of ALPR images for which no independent records exist outside the Vigilant user interface.

In contrast with the other reviewed agencies, Los Angeles has limited its sharing of ALPR images to entities within a regional structure established for its ALPR program through a federal grant that helped fund its ALPR program. As Figure 5 shows, Los Angeles shares ALPR images with 58 other law enforcement agencies in the region. It does not have agreements to share its ALPR images with any federal agencies, including ICE. According to the lieutenant who administers the ALPR program, Los Angeles decided to share images only with entities using the same software so that it could maintain greater control over its ALPR images. It has a formal agreement with each agency, which provides a record of its sharing decisions.

Figure 5
Los Angeles Shares Images With 58 Law Enforcement Agencies



Source: Analysis of data-sharing memorandums of agreement.

The Agencies' Image Retention Decisions Are Unrelated to How They Use the Images

The four agencies we reviewed retain ALPR images for varying periods of time. Our review determined that with the exception of CHP, state law does not mandate a specific retention period for ALPR images collected, accessed, or used by public agencies, nor does state law delineate the factors public agencies should use in determining those periods. Instead, state law requires that public agencies other than CHP that use or operate ALPR systems specify, in the agency's usage and privacy policy, the length of time ALPR data will be retained and the process that the agency will use to determine if and when to destroy retained ALPR data. Fresno's policy is to retain ALPR images for a minimum of one year, Sacramento's policy is to retain ALPR images for a minimum of two years, and Marin's policy is to retain images for two years. Although the agencies' policies describe their retention periods as minimums, in practice the agencies have configured their ALPR systems to delete images older than their specified retention periods. Fresno and Sacramento each download and retain images for longer than their prescribed retention policies if the images are relevant to investigations. Los Angeles does not have an ALPR policy, but the lieutenant who administers the ALPR program stated that it adheres to the city's Administrative Code, which requires data to be retained for a minimum of five years.

None of the agencies considered the images' utility over time when establishing their retention periods.

None of the agencies considered the images' utility over time when establishing their retention periods. Fresno based its ALPR image retention period on state law, which allows some cities to destroy certain video monitoring records after one year. Marin did not cite state law in its policy; its former ALPR administrator stated that when setting a two-year retention period, he considered other agencies' retention periods and the retention requirements for litigation related to investigations. Both Marin's and Fresno's ALPR administrators stated that they were not aware of any studies of how useful older images in their ALPR systems were to their personnel. In its ALPR policy, Sacramento cited a general state law that prohibits some cities from destroying records less than two years old. The lieutenant who oversees Sacramento's ALPR program acknowledged that the agency has not conducted any statistical analysis to determine how long it needs to retain ALPR images. However, he stated that, although he was not involved in drafting the original policy, two years made sense considering federal regulations, which permit retention of criminal intelligence information for no longer than five years. The lieutenant cited those federal regulations as a best practice for retaining sensitive data, connecting the ALPR images to a tenet of federal regulations that law enforcement agencies should keep criminal intelligence information as long as it is useful, even though ALPR data are not criminal intelligence.

To develop a retention policy that better protects individuals' privacy, an agency might begin by considering the time period during which ALPR data are most useful to law enforcement. To assess the usefulness of these images over time, we reviewed the four agencies' ALPR searches over a six-month period—between late January and September 2019, depending on when we visited the agencies—and found that personnel at three of the four agencies typically searched for ALPR images zero to six months old. When searching ALPR systems, investigators can enter search dates to target specific periods of interest. For example, on March 29, 2019, a Sacramento investigator searched for ALPR images from six days earlier—March 23—indicating that images less than one week old were relevant to that search. As Table 2 shows, we found that the searches agency personnel at the three agencies performed infrequently included older images. In fact, when investigators at Fresno, Marin, and Sacramento specified date ranges, most searches were of ALPR images that were less than six months old. In contrast, Los Angeles had a relatively even distribution of searches between those less than one year and those more than one year old. The Vigilant system defaults to showing the 50 most recent records when investigators do not specify a search date range. We analyzed 46,000 records for searches that did not specify a date range and found that investigators for Marin, Fresno, and Sacramento frequently did not seek further than the 50 default records, indicating that they generally were not interested in older ALPR images.

Table 2
The Agencies Usually Search for ALPR Images That Are Six Months Old or Less

			PERCENTAGE OF SEARCHES FOR IMAGES OF A SPECIFIED AGE			
	RETENTION PERIOD	TOTAL SEARCHES OVER 6-MONTH PERIOD ANALYZED	0 TO 6 MONTHS	6+ MONTHS TO 1 YEAR	1+ TO 2 YEARS	MORE THAN 2 YEARS
Fresno*	1 year	850	92%	6%	1%	1%
Los Angeles	**5 years**	28,874	42	8	29	21
Marin*	2 years	26	88	8	0	4
Sacramento*	2 years	4,262	84	4	11	1

Source: Analysis of search records from the agencies' ALPR systems between late January and September 2019, depending on when we visited the agency.

* The percentage of searches listed in this table beyond an agency's retention period are likely from their personnel searching data belonging to other agencies with longer retention periods.

Other states have established retention periods that are generally shorter than the lengths of time California's local law enforcement agencies are retaining ALPR images. The National Conference of State Legislatures identified at least 13 states that mandate maximum ALPR image retention periods. As the text box shows, these vary widely, from three minutes in New Hampshire to three years in Florida. Nevertheless, the majority of these states have retention periods that do not exceed six months.

In contrast, 230 California agencies responding to our survey reported that they use ALPR systems, and nearly 80 percent of these—180 agencies—stated that they retain their ALPR images for more than six months. About 20 of those agencies indicated that they retain ALPR images for more than five years. Figure A.2 in Appendix A summarizes these responses.

ALPR Image Retention Periods for 13 States

New Hampshire	***3 minutes***
Maine	21 days
Minnesota	60 days
Montana	90 days
North Carolina	90 days
Tennessee	90 days
Arkansas	150 days
Nebraska	180 days
-------- **LONGER THAN SIX MONTHS** --------	
Utah	270 days
Colorado	365 days
Vermont	540 days
Georgia	900 days
Florida	***3 years***

Source: National Conference of State Legislatures, *Automated License Plate Readers: State Statutes,* March 15, 2019, and review of the listed states' ALPR laws and guidelines.

Note: These states allow retention for longer periods for specific reasons, such as data used in investigations.

The length of time law enforcement agencies need to retain ALPR images will vary depending on how they use the images. Narrow use—for one purpose only, such as locating stolen cars—could dictate a short retention window. Personnel we interviewed at each of the four agencies stated that investigators rely primarily on recent images to investigate some types of crimes, such as auto theft. In contrast, using ALPR images to solve complex crimes could necessitate a longer retention window. For example, first-degree murder can be prosecuted at any time; therefore, a homicide investigator may be able to use ALPR images of any age to help solve a case. The four agencies we reviewed have access to information they can use to evaluate whether their ALPR retention periods are reasonable. Their systems record each time personnel search ALPR images, and these search records show the date of the search and the parameters used to narrow the search, such as location, date, and time. Agency administrators can analyze these activity logs to understand the images personnel are searching for and their relative ages.

Marin and Sacramento have allowed expired hot lists to remain in their ALPR systems for far longer than their specified retention periods. Unlike ALPR images, hot lists cannot be automatically deleted by the Vigilant system. Instead, the agencies define a period after which the hot list becomes inactive—meaning the ALPR system no longer generates alerts from the list—but the list remains stored in Vigilant's servers until the agency deletes it. We found that Marin and Sacramento are retaining hot lists longer than necessary because their administrators were unaware of the need to manually delete them. They assumed that their Vigilant system would automatically delete inactive hot lists according to the designated purge schedule, as it does ALPR images. For example, Marin retained an inactive hot list of sex offenders for five years—three years longer than its two-year retention period for ALPR images. Sacramento has retained multiple hot lists for as long as six years—four years longer than its retention period for ALPR images. The types of lists ranged from a hot list of Sacramento County sex offenders to a warrants hot list. When we brought the inactive hot lists to the agencies' attention,

the administrators at Marin and Sacramento acknowledged that the age of the hot lists exceeded the agency's retention period, and they were willing to delete the hot lists.

Law enforcement agencies should consider both the usefulness of the ALPR images and individuals' privacy when deciding how long to retain the images. Cost, however, is not a factor. According to the lieutenant who oversees Los Angeles' ALPR program, the images are useful to investigators and the cost of storing ALPR images is not a significant factor in determining how long to store them. Nevertheless, two studies by a consultant to the National Institute of Justice and the chiefs' association concluded that law enforcement agencies must consider the trade-offs between privacy concerns and the utility of retaining the ALPR images they capture and store.

The Law Enforcement Agencies Have Failed to Monitor Use of Their ALPR Systems and Have Few Safeguards for Creating ALPR User Accounts

Instead of ensuring that only authorized users access their ALPR data for appropriate purposes, the agencies we reviewed have made abuse possible by neglecting to institute sufficient monitoring. ALPR systems should be accessible only to employees who need the data and who have been trained in using the system. However, the agencies often neglected to limit ALPR system access, to provide appropriate training to individuals with access, or to monitor accounts. Similarly, to ensure that individuals with access do not misuse the system, the agencies should audit the license plate searches users perform. Instead, the agencies conduct little to no auditing and thus have no assurance that misuse has not occurred.

Best Practice Safeguards for Establishing and Managing User Accounts

Account Setup

- Supervisor approval is a prerequisite for account access.
- ALPR training is a prerequisite for account access.

Account Maintenance

- Accounts defined as *inactive* are suspended.
- ALPR training is required for users linked to inactive accounts to regain active status.
- Accounts are deleted when employees separate from the agency.

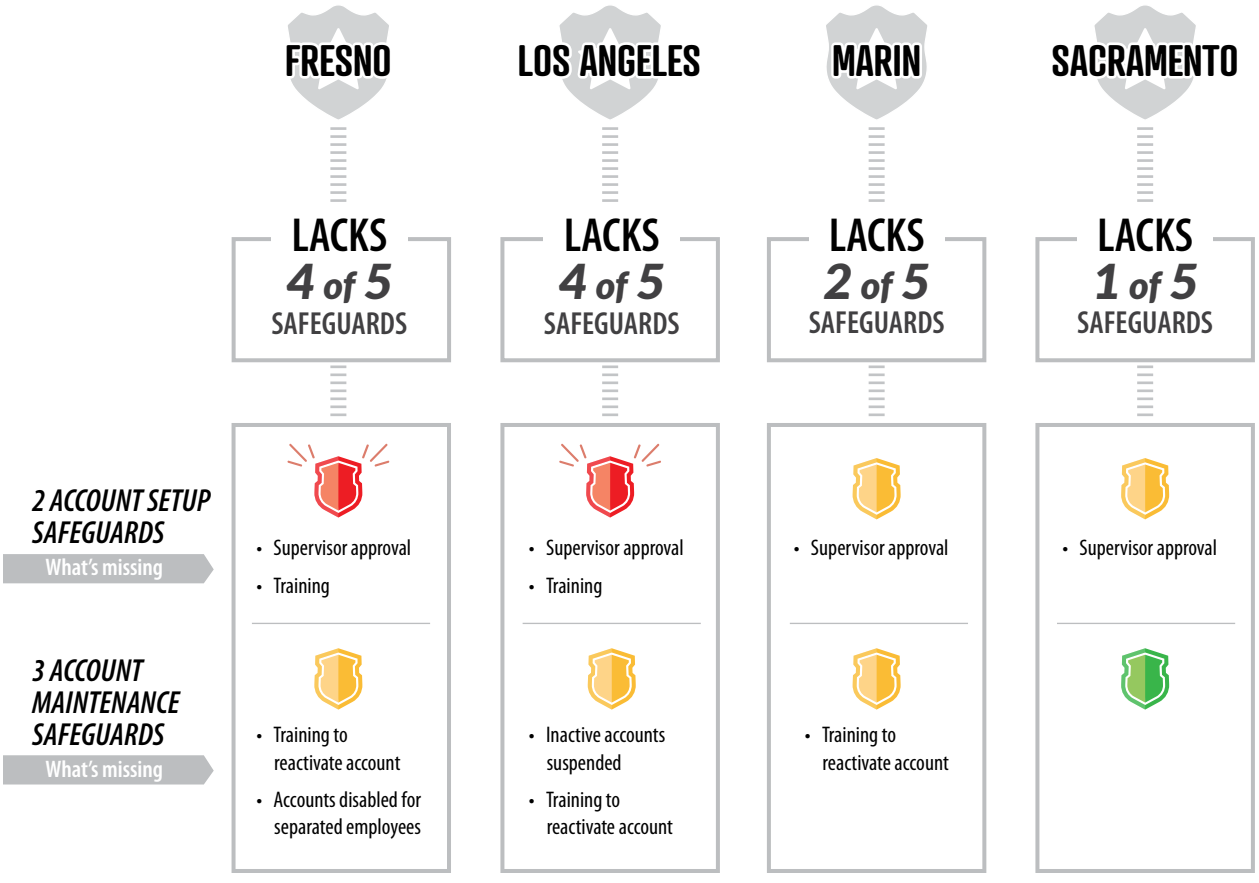
Source: CJIS policy and the *State Administrative Manual*.

The Agencies Need Stronger User-Access Safeguards

The four agencies we reviewed all failed to follow one or more best practices related to user access. State law requires agencies to maintain reasonable security procedures and practices to protect ALPR data from unauthorized access, and the text box lists five best practices for user access, from initiating an account to disabling it when an employee separates from the agency. Figure 6 shows the four agencies' status in implementing these best practices. Each ALPR administrator stressed the concept of "need to know, right to know" as a key for data security; however, no agency followed all of the best practices that would help establish the need to know and right to know. For example, no agency had a requirement

that supervisors approve staff requests for creating ALPR user accounts. Such a step would provide assurance that the staff member receiving the account had both a need and a right to access the information in the ALPR system. Los Angeles is particularly lax in this area because the protocol of its IT division is to include its ALPR software on each computer it assigns to staff, regardless of their position. Thus, staff who do not perform functions related to the ALPR system nevertheless have access to the system. In contrast, Sacramento follows all but one of the best practices listed in the text box. In doing so, it requires staff to prove their initial and continued need for ALPR data, among other access requirements.

Figure 6
The Agencies Lack Many Best Practice Safeguards for Establishing and Managing User Accounts



Source: Agencies' policies, applicable procedures and protocols, and interviews with the agencies' management.

Agencies could reduce instances of unnecessary access by ensuring that only those staff whose current work assignments require access to ALPR data have that access. The ALPR administrators at Marin and Los Angeles believe that supervisory approval is unnecessary

because ALPR users are already privy to data they consider more confidential than ALPR data, such as criminal justice information. However, these views do not consider that ALPR systems capture images indiscriminately, irrespective of the criminal history of the individual who is driving the vehicle, and the images allow law enforcement to track individuals. Given that agencies retain these images for several months or years, a user could combine them with personal information from separate data sources to produce a great number of details about someone's life, such as his or her political or religious affiliation. Without proper safeguards, staff could conduct this form of surveillance on any driver. In fact, the chiefs' association acknowledged this possibility and warned that increasing ALPR use and data sharing would enhance the potential for surveillance. Thus, as the chiefs' association concluded, limiting ALPR access to employees with the needs and the rights to access these data is a good step toward protecting the individuals whose privacy would be violated if the data were misused.

Limiting ALPR access to employees with the needs and the rights to access these data is a good step toward protecting the individuals whose privacy would be violated if the data were misused.

Ensuring that ALPR users are properly trained is another weakness among the agencies we reviewed. Three of the agencies do not ensure that all of their ALPR users are properly trained. The chiefs' association called the training of authorized ALPR users "a critical accountability measure." However, as Figure 6 shows, neither Fresno nor Los Angeles requires all ALPR users to complete ALPR training before initially obtaining system access. Although Los Angeles offers ALPR training, the detective who conducts this training confirmed that it is not required before users can access the ALPR system. Fresno's policy encourages such training; however, its ALPR administrator confirmed that the agency does not provide training to all of its users. Further, Marin's ALPR administrator stated that although Marin provides training when staff first receive access to the ALPR system, it does not require staff to renew their training in order to reactivate their accounts following long periods of not using the system. Without sufficient training, there is little assurance that ALPR users know and understand agency ALPR policies, including recent changes, or are aware of the limits on how they may use ALPR data.

Although the Fresno ALPR administrator agrees that the agency's safeguards surrounding user access are currently inadequate and plans to improve them, the ALPR administrators at Los Angeles, Marin, and Sacramento believe their current practices are acceptable. The administrators at Marin and Los Angeles are reluctant to alter their agencies' existing practices because they believe ALPR data are not as sensitive as other law enforcement data. We disagree with these views because, as we mention previously, ALPR data are sensitive and state laws require reasonable security procedures and practices to protect them. A basic protection for data that must be treated as sensitive is to limit who can access them.

In addition, as we mention earlier, the ALPR images law enforcement agencies collect largely involve vehicles that are not associated with crimes, and if the images were analyzed, the data could reveal behavior patterns and preferences that law enforcement could use to conduct surveillance on individuals. For example, according to a 2012 newspaper article, the New York Police Department collected license plate numbers of vehicles parked near a mosque. The department was purportedly trying to identify terrorist activities. Although the department justified this data collection as part of its strategy to identify potential criminal activities, it targeted mosques and collected license plate numbers at times without any leads or proof of terrorist connections. Given the sensitivity of the information collected in this example, access safeguards would ensure that only those staff who have a need and right to access an ALPR system would possess that privilege.

Law enforcement agencies could further improve safeguards by disabling employees' accounts once they separate or after long periods of nonuse. We reviewed Marin's and Sacramento's processes for disabling accounts of separated employees. Both agencies follow a similar approach, relying on one part of the organization providing information to another. Sacramento produces a personnel transfer and separation list every two weeks, and the IT security group uses it to identify accounts to close. Although the IT security group generally disabled accounts promptly after receiving the list, we found that the contents of the list were not always current. For example, in one instance, a separated employee did not appear on the list until 46 days after his separation date in June 2019. According to a human resources specialist, employees submit their resignation paperwork late at times, which causes human resources to not process this paperwork until after an employee has left the department. Marin's ALPR administrator said that he removes ALPR accounts once he receives a department-wide email notifying him of an employee's resignation or termination. He also stated that he checks ALPR accounts every few months to verify that active accounts match active employees. However, for one employee, the administrator did not disable his ALPR access until two months after he resigned in October 2019. In fact, the administrator did not disable this employee's access until our office pointed out that the account was still active. The fact that Marin and Sacramento did not disable some accounts as necessary is problematic because the former employees could log into their accounts and access ALPR data from the web-based version of the ALPR systems on any Internet-capable device, not just office devices.

The fact that Marin and Sacramento did not disable some accounts as necessary is problematic because the former employees could log into their accounts and access ALPR data from the web-based version of the ALPR systems on any Internet-capable device, not just office devices.

With regard to Los Angeles and Fresno, Los Angeles' network manager described an automated process for deleting accounts linked to overall network access, which reasonably aligned with best practices. Conversely, Fresno's ALPR administrator said that

he periodically reviews the names of employees with user accounts but started doing so only in September 2019 when he learned of our audit. We did not test deleted accounts at either agency. Deleting accounts prevents separated employees from continuing to access ALPR data and is thus critical to protecting ALPR data and individuals' privacy.

The Agencies Have Failed to Audit ALPR Users' Searches to Ensure That Individuals' Privacy Is Protected

State law requires law enforcement agencies that operate, access, or use ALPR systems to protect their ALPR data—including ALPR images—from unauthorized access, destruction, use, modification, or disclosure. The law specifically requires them to describe and implement a policy detailing how they will monitor their ALPR systems. According to state law, agencies that access or use ALPR systems must also conduct periodic system audits. In its reports on managing ALPR systems, the chiefs' association stated that conducting audits aids in discouraging unnecessary or inappropriate use of the data; in addition, when agency policies include a strong auditing requirement, this reassures the public that their privacy interests are recognized and respected.

Even though law enforcement agencies that use or access ALPR systems can monitor searches simply by reviewing search records for red flags, they should also conduct audits as required by state law.

A primary form of auditing to prevent misuse is reviewing the searches users conduct in the ALPR systems. Users conduct searches for specific license plates. Even though law enforcement agencies that use or access ALPR systems can monitor searches simply by reviewing search records for red flags, such as an unknown user account, they should also conduct audits as required by state law. An audit entails a more rigorous approach, including evaluating risk and randomly selecting test items for review. Developing an audit of license plate searches, for example, would involve determining how many searches to review, how to select test items, and how frequently to conduct the audit. Law enforcement agencies have often found evidence of misuse of their databases, showing the need for auditing. For example, a news article reported that CHP investigated 11 cases of database misuse in 2018, including three involving officers improperly looking up information on license plates through CLETS without a need to know the information. The large datasets of ALPR images, dating back at least one year, that the four reviewed agencies maintain can be analyzed to reveal the daily patterns of vehicles that can be linked to individuals and their activities—most of whom have not engaged in criminal activity. A member of law enforcement could misuse ALPR images to stalk an individual or observe vehicles at particular locations and events, such as doctors' offices or clinics and political rallies. Despite these risks, the agencies we reviewed conduct little to no auditing of users' searches.

We asked key officials at the three agencies using the Vigilant system why they had not audited the searches users performed and found that either they were unaware of the auditing requirement in state law or the auditing they did conduct did not include user searches. Fresno's policy states that it should conduct audits on a regular basis, but the ALPR administrator told us he believed audits are the responsibility of the Audits and Inspections Division within the department. However, the sergeant responsible for audits and inspections—who took charge in January 2018—responded that he was not aware of the requirement until our audit. Similarly, the Marin ALPR administrator was unaware of the state law requiring audits of ALPR systems until our audit and thus had not been conducting them. At Sacramento, the policy states that the ALPR administrator will conduct periodic audits of user searches. Even though Sacramento administrators had been monitoring some system functions, they had not audited searches of the older ALPR images. The officer administering the ALPR program until April 2019 said that she did not conduct these audits because her predecessor had not informed her that it was necessary. The ALPR program transferred to a new division in April, and according to the current ALPR administrator, limited staff resources have prevented him from instituting these audits.

Although the agencies have not been conducting audits, we considered the possibility that an agency employee or member of the public may have reported instances of ALPR misuse. We searched each agency's records of internal affairs investigations from January 1, 2016, to the present for cases involving ALPR misuse and did not find any such cases. However, we do not consider this proof that no instances of ALPR misuse occurred. Given that the agencies were not regularly auditing their systems, ALPR misuse may have occurred and gone unnoticed and unreported.

All four agencies must address the quality of information they will need to audit user searches. In Sacramento, for 66 percent of searches, users left case number and search reason fields blank.

To engage in meaningful auditing of their system users, all four agencies need to address the quality of the information users enter into the system as part of their searches. Before allowing users to conduct searches, Fresno, Los Angeles, and Marin require users to enter case numbers and reasons for the search; however, this is not happening consistently. We reviewed six months of user queries at the three agencies and found that users entered a wide variety of information in the case number field. For example, users at Los Angeles simply entered "investigation" into this field as well as descriptions of vehicles and actual case numbers. In contrast, Sacramento does not require users to enter either case numbers or reasons. Our review showed that in 66 percent of searches, Sacramento's users left both fields blank. When users fail to enter any information or fail to include appropriate detail, identifying misuse through audits becomes nearly impossible.

Los Angeles faces additional hurdles in performing meaningful auditing because its ALPR administrators do not have immediate access to data on user searches. Instead, according to the chief data officer, administrators need to request that a software engineer from Los Angeles' ALPR software contractor build and run a query in the system to obtain these data. In 2015 Los Angeles recognized a need to fix this software limitation to enable administrators to audit user searches. The chief data officer for Los Angeles stated that, although an initial upgrade provided an audit dashboard tool for administrators, subsequent software upgrades made this tool unusable, and the company that provides the software is developing a new one. He said that it is Los Angeles' goal to have a new audit dashboard tool by the end of the first quarter of 2020, at which point he will work with the appropriate division within the department to develop an audit plan. Although we agree that an audit tool will facilitate audits, we believe it was entirely possible for Los Angeles to obtain the data on user searches, and thus it could have implemented a process for periodic system audits as state law requires, despite the difficulties.

Fresno, Marin, and Sacramento do not have adequate policies or processes in place for conducting meaningful audits.

The other three agencies also do not have an adequate policy or process in place for conducting meaningful audits. For example, Fresno's ALPR policy states that it should conduct periodic audits, but its policy does not specify how frequently it will audit its ALPR system, who will perform those audits, who will review and approve the audit results, and how long it will retain the audit documents. Specifics such as these provide a clear road map for planning, conducting, documenting, and resolving audits. When followed, the agencies will have records demonstrating their necessary oversight. Marin's latest policy—dated July 2019—also fails to cover these necessary details. Fresno and Marin began reviewing user queries subsequent to the beginning of our audit, but in the absence of an adequate policy or formal plan, their methodologies are lacking. For example, although Fresno began conducting audits that included a random sample of user searches, staff have not developed a formal plan and provided us only with handwritten notes on their methodology. Marin's ALPR administrator has not instituted audits and is simply monitoring license plate searches by looking for instances in which the user did not enter a reason for the search or entered a reason that does not make sense, such as an investigation that does not exist. In addition, at both Fresno and Marin, the individual conducting the audits or monitoring is also a system user, creating a conflict when acting as a system monitor or auditor. Without sound methodologies, the agencies cannot be confident that they have sufficient protocols in place to detect misuse.

Other Areas We Reviewed

To address all the audit objectives approved by the Joint Legislative Audit Committee (Audit Committee), we reviewed two additional subject areas: whether the agencies offered opportunities for the public to comment on their ALPR programs and whether the Sacramento County Department of Human Assistance (Human Assistance) continues to operate an ALPR program.

Three Agencies Provided Information to the Public on Their ALPR Programs

State law requires that public agencies implementing ALPR programs after January 1, 2016, offer an opportunity for the public to comment about those programs. These opportunities increase public awareness that law enforcement agencies are using electronic means to collect information about vehicles in the community and offer a way for the public to provide feedback about the programs. The four agencies we reviewed began using ALPR before 2016 and consequently were not required to offer an opportunity for public comments. Nonetheless, three of the agencies took some steps to communicate with the public about their ALPR programs. Los Angeles and Sacramento published documents describing their ALPR programs, and at a Fresno City Council meeting, the public had an opportunity to comment on the selected ALPR vendor before the council voted on a new contract. The minutes from that meeting reflect that the public made no comments. This transparency helps foster public trust in law enforcement and government as a whole.

Human Assistance No Longer Operates an ALPR Program

Our audit scope included reviewing the ALPR program of Human Assistance, which provides Sacramento County residents with employment assistance and supportive services. Human Assistance contracted with Vigilant for three years to access ALPR images. Human Assistance did not operate its own cameras, and it used the ALPR images to investigate welfare fraud. According to the administrator of its ALPR program, Human Assistance ended its program in 2018 after determining that investigative staff rarely searched the images, so the program could not justify the cost. On November 1, 2018, Human Assistance deleted its ALPR user accounts, leaving the administrator's account active for internal review. On May 31, 2019, Human Assistance's ALPR agreement with Vigilant expired, and the administrator no longer has access to the account. Therefore, we did not perform any additional audit work pertaining to Human Assistance.

Recommendations

Legislature

- To better protect individual's privacy and to help ensure that local law enforcement agencies structure their ALPR programs in a manner that supports accountability for proper database use, the Legislature should amend state law to do the following:
  - Require Justice to draft and make available on its website a policy template that local law enforcement agencies can use as a model for their ALPR policies.
  - Require Justice to develop and issue guidance to help local law enforcement agencies identify and evaluate the types of data they are currently storing in their ALPR systems. The guidance should include the necessary security requirements agencies should follow to protect the data in their ALPR systems.
  - Establish a maximum data retention period for ALPR images. The Legislature should also establish a maximum data retention period for data or lists, such as hot lists, that are used to link persons of interest with license plate images.
  - Require periodic evaluation of a retention period for ALPR images to ensure that the period is as short as practicable.
  - Specify how frequently ALPR system use must be audited and that the audits must include assessing user searches.
  - Specify that those with access to ALPR systems must receive data privacy and data security training. The Legislature should require law enforcement agencies to include training on the appropriateness of including certain data in an ALPR system, such as data from CLETS.

Law Enforcement Agencies

- To ensure that their ALPR policies contain all of the required elements as specified in state law, by August 2020, Fresno, Los Angeles, Marin, and Sacramento should review their policies and draft or revise them as necessary. Also by August 2020 these agencies should post their revised policies on their websites in accordance with state law.

- To protect ALPR data to the appropriate standard, Fresno, Los Angeles, Marin, and Sacramento should do the following:
  - By August 2020, identify the types of data in their ALPR systems and, as they review or draft their ALPR policies, ensure that they clarify the types of information their officers may upload into their ALPR systems, such as, but not limited to, information obtained through CLETS.
  - By August 2020, perform an assessment of their ALPR systems' data security features, and make adjustments to their system configurations where necessary to comply with CJIS policy best practices based on that assessment.
- To ensure that the agreements with their cloud vendor offers the strongest possible data protections, by August 2020, Fresno, Marin, and Sacramento should enter into new contracts with Vigilant that contain the contract provisions recommended in CJIS policy.
- To ensure that ALPR images are being shared appropriately, the specific agencies noted should do the following:
  - By April 2020, Fresno, Marin, and Sacramento should review the entities with which they currently share images, determine the appropriateness of this sharing, and take all necessary steps to suspend those sharing relationships deemed inappropriate or unnecessary.
  - As Los Angeles develops its ALPR policy, it should be certain to list the entities with which it will share ALPR images and the process for handling image-sharing requests.
  - By August 2020, Marin and Sacramento should each develop a process for handling ALPR image-sharing requests that includes maintaining records separate from the Vigilant system of when and with whom they share images. The process should verify a requesting agency's law enforcement purpose for obtaining the images and consider the requesting agency's need for the images. The process should be documented in the agency's ALPR policy and/or procedures.
  - By August 2020, Fresno should revise its written procedures for ALPR image-sharing, as necessary, to ensure that it follows those procedures.

- To minimize the privacy risk of retaining ALPR images for long periods of time, Fresno, Los Angeles, Marin, and Sacramento should do the following:

  - By August 2020, review the age of the ALPR images their personnel are searching for and ensure that their retention periods for ALPR images are based on department needs. Each agency should reflect in its ALPR policy the updated retention period and state in its policy that it will reevaluate its retention period at least every two years.

  - Include in their ALPR policies a retention period for data or lists, such as hot lists, used to link persons of interest with license plate images, and create necessary processes to ensure that those data unrelated to ongoing investigations are periodically removed from their ALPR systems.

- To ensure that ALPR system access is limited to agency staff who have a need and a right to use ALPR data, Fresno, Los Angeles, Marin, and Sacramento should do the following:

  - By April 2020, review all user accounts and deactivate accounts for separated employees, inactive users, and others as necessary.

  - Ensure that their ALPR policies specify the staff classifications, ranks, or other designations that may hold ALPR system user accounts and that accounts are granted based on need to know and right to know.

  - By August 2020, develop and implement procedures for granting and managing user accounts that include, but are not limited to, requiring that supervisors must approve accounts for users, providing training to users before granting accounts, suspending users after defined periods of inactivity, and requiring regular refresher training for active users and training for users before reactivating previously inactive accounts. Each agency should also ensure that it has procedures in place to deactivate an account immediately for an account holder who separates from the agency or who no longer needs a user account.

- To enable auditing of user access and user queries of ALPR images, Fresno, Los Angeles, Marin, and Sacramento should do the following:

  - By April 2020, assess the information their ALPR systems capture when users access them to ensure that the systems' logs are complete and accurate and that they form a reasonable basis for conducting necessary, periodic audits.

  - Ensure that their ALPR policies make clear how frequently they will audit their ALPR systems, who will perform those audits, who will review and approve the audit results, and how long they will retain the audit documents. Each agency should have in place by February 2021 an audit plan that describes its audit methodology, including, but not limited to, risk areas that will be audited, sampling, documentation, and resolution of findings.

  - By June 2021, implement their audit plans and complete their first audits.

We conducted this performance audit under the authority vested in the California State Auditor by Government Code 8543 et seq. and in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Respectfully submitted,

ELAINE M. HOWLE, CPA
California State Auditor

February 13, 2020

Blank page inserted for reproduction purposes only.

Appendix A

Summary of ALPR Survey Responses

The Audit Committee requested that we determine ALPR use among law enforcement agencies statewide. Specifically, the Audit Committee asked us to determine whether agencies use ALPR information, what vendors they use, and whether law enforcement agencies have policies and procedures to govern their use and sharing of ALPR information. We surveyed 391 county sheriffs and municipal police departments statewide. We relied upon information from the California State Sheriffs' Association, the California Police Chiefs Association, and the FBI to obtain assurance that our list of statewide local law enforcement was reasonably comprehensive.

Agencies That Did Not Respond to Our Survey

- Anderson Police Department
- Barstow Police Department
- Del Norte County Sheriff's Office
- Lakeport Police Department
- Lodi Police Department
- Mendocino County Sheriff's Office
- Mount Shasta Police Department
- Oceanside Police Department
- San Francisco Sheriff's Department
- Siskiyou County Sheriff's Department

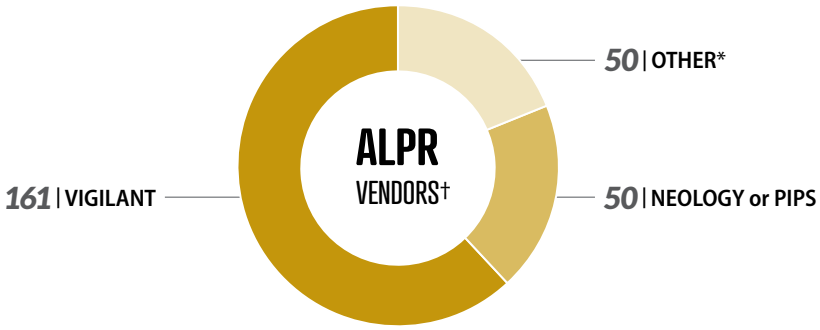
Source: Analysis of survey responses.

We received 381 responses (97 percent) to the 391 surveys we sent. Ten agencies we surveyed did not respond. The text box lists those agencies. A breakdown of the law enforcement agencies' responses to our statewide survey can be found at http://auditor.ca.gov/reports/2019-118/supplemental.html. The discussion here summarizes the survey results.

Summary of Results From Agencies That Reported Using ALPR Systems

In responding to our survey, law enforcement agencies indicated whether they use ALPR systems and, if so, what vendors' systems they use to collect and access ALPR information. Of the agencies that responded, 60 percent, or 230 agencies, reported that they currently operate or access information from ALPR systems. Of those agencies, 96 percent said they have an ALPR usage and privacy policy. Vigilant is the most common vendor for the agencies that reported using ALPR systems. Figure A.1 summarizes which vendors the 230 law enforcement agencies reported that they use. Finally, 9 percent, or 36 of the agencies we surveyed, stated that they are implementing or planning to implement ALPR systems.

Figure A.1
Vigilant Is the ALPR Vendor the Majority of Law Enforcement Agencies Use



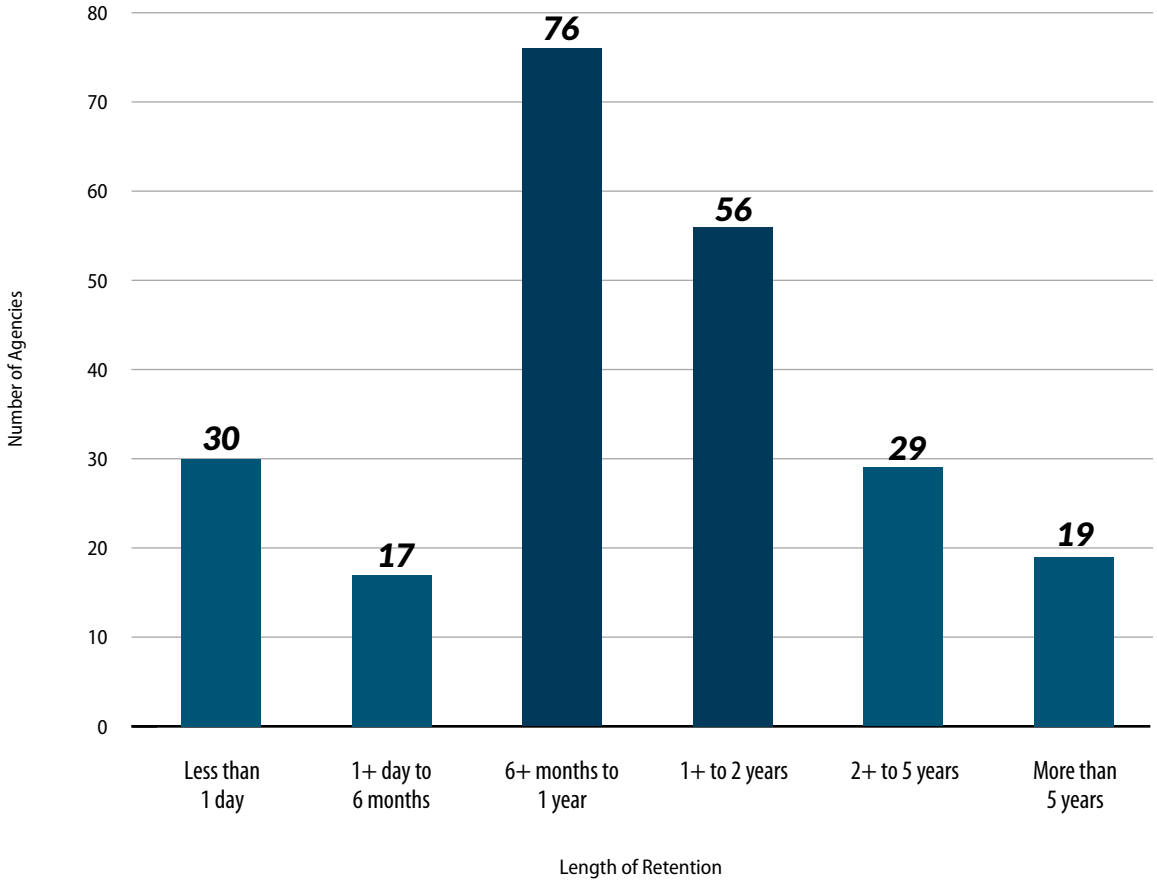
Source: Analysis of survey responses.

* The *Other* category includes vendors such as Genetec, ELSAG, and All Traffic Solutions.

† The total number of ALPR vendors used is greater than the 230 agencies that said they use ALPR systems because some agencies use more than one vendor.

Law enforcement agencies that reported using ALPR systems also answered questions related to their retention and sharing of ALPR information. We asked how long the agencies retain ALPR information not related to ongoing investigations or litigation. As Figure A.2 shows, the retention periods varied, but the majority of law enforcement agencies reported retention periods between six months and two years. Additionally, we asked agencies that operate ALPR systems if they share or sell the information they collect with other law enforcement or public agencies. Seventy-three percent, or 168 agencies that use ALPR systems, reported that they share ALPR images with other law enforcement agencies; only three of those agencies also reported that they share ALPR images with other public agencies that are not law enforcement. None of the agencies we surveyed reported selling images to other law enforcement or public agencies.

Figure A.2
A Majority of Agencies Generally Retain ALPR Information for Between Six Months and Two Years



Source: Analysis of survey responses.

Note: Three responding agencies that use ALPR systems did not indicate a retention period for their information: Bakersfield Police Department, Fountain Valley Police Department, and Pasadena Police Department.

Blank page inserted for reproduction purposes only.

Appendix B

Scope and Methodology

The Audit Committee directed the California State Auditor to conduct an audit of the extent to which local law enforcement agencies are complying with existing law regarding the use of ALPR systems. The analysis the Audit Committee approved contained five objectives. We list the objectives and the methods we used to address them in Table B.

Table B
Audit Objectives and the Methods Used to Address Them

	AUDIT OBJECTIVE	METHOD
1	Review and evaluate the laws, rules, and regulations significant to the audit objectives.	Reviewed relevant state laws, regulations, and other background materials applicable to the use and operation of ALPR systems by local law enforcement.
2	To the extent possible, determine the following for law enforcement agencies statewide: a. Whether they use ALPR information and, if so, what vendors they use to access this information. b. Whether they have policies and procedures in place governing the use and sharing of ALPR information.	• Surveyed 391 county sheriff and municipal police departments statewide. • Obtained and verified a list of statewide local law enforcement agencies, using information from the California State Sheriffs' Association, the California Police Chiefs Association, and the FBI. • Questioned agencies regarding their use of ALPR systems, including whether they use or are planning to use an ALPR system; if they share or sell the ALPR information; if their ALPR storage is CJIS-compliant; which system they use to store, share, or access ALPR information; if they have a usage and privacy policy and post the policy on their website; how long they retain ALPR information; how many department personnel have access to the ALPR data; and how many total personnel their department has. Full questions and a breakdown of the responses are on our website at http://auditor.ca.gov/reports/2019-118/surveys.html. • Created an interactive graphic to display responses by county, assembly district, and senate district at http://auditor.ca.gov/reports/2019-118/supplemental.html. • The survey responses were self-reported, and we did not verify their accuracy.

continued on next page . . .

	AUDIT OBJECTIVE	METHOD
3	Examine the use of ALPRs by the Sacramento County Sheriff's Office and Department of Human Assistance, the Los Angeles Police Department, the Fresno Police Department, and the Marin County Sheriff's Office by performing the following:	
	a. Determine whether they have policies and procedures in place regarding ALPR systems and whether those policies contain the elements state law requires.	• Interviewed the agencies' ALPR administrators. • Obtained and reviewed ALPR policies and procedures and determined whether each agency met state law requirements in this area.
	b. Determine whether they have followed state law regarding all required public notifications related to ALPR systems and information, including required public hearings.	• Interviewed the agencies' public information officers. • Obtained evidence of public notifications and public hearings and determined whether each agency met state requirements in this area.
	c. Determine whether they maintain records of access to ALPR information from both within and outside the agency that includes all required documentation and whether they have ensured that ALPR information has only been used for authorized purposes.	• Interviewed the agencies' ALPR administrators. • Reviewed access records from the agencies' ALPR systems. • Determined whether the agencies conducted any audits or monitoring by interviewing ALPR administrators, staff of internal audit divisions, and executive staff of any oversight entities. We also reviewed relevant policies and procedures. • Reviewed the agencies' internal affairs files for any cases involving ALPR misuse. • Reviewed Justice's and the FBI's audits of the agencies' IT security and the safeguards those audits identified.
	d. Determine whether they have sold, shared, or transferred ALPR information only to other public agencies, except as otherwise permitted by law, and whether they have properly documented these activities.	• Interviewed the agencies' ALPR administrators. • Reviewed reports and records about data sharing from the agencies' ALPR systems. • Reviewed existing memorandums of agreement and understanding for data sharing. • Interviewed executive staff at Vigilant regarding ALPR system functionality and their procedures for verifying the law enforcement purpose of client agencies.
	e. Determine the nature of any contracts with third-party vendors related to ALPR information.	• Interviewed Justice staff responsible for protecting criminal justice information. • Evaluated the agencies' contracts with third-party vendors and determined whether the contracts contained adequate protections for information in the agencies' ALPR systems.
4	Evaluate whether current state law governing ALPR programs can be enhanced to further protect the privacy and civil liberties of California residents.	• Interviewed agencies' investigators and ALPR program administrators. • Reviewed the information in the agencies' ALPR systems and identified the necessary protections for that information. • Obtained the agencies' justifications for their ALPR data retention periods. • Analyzed six months of the agencies' ALPR search records— between late January and September 2019, depending on when we visited the agencies—to determine how often the agencies' personnel searched for older data in their ALPR systems. • Reviewed other states' ALPR data retention laws based on a report from the National Conference of State Legislatures and identified best practices for data retention. • Analyzed laws pertaining to privacy, personal information, and criminal justice information and determined whether changes to current ALPR law would further protect the privacy and civil liberties of California residents.
5	Review and assess any other issues that are significant to the audit.	Reviewed informational material produced by law enforcement agencies, nonprofit organizations, and other entities to identify concerns surrounding privacy and ALPR systems.

Source: Analysis of state law, policies, information, and documentation identified in the table column titled Method.

Assessment of Data Reliability

The U.S. Government Accountability Office, whose standards we are statutorily obligated to follow, requires us to assess the sufficiency and appropriateness of computer-processed information that we use to support our findings, conclusions, and recommendations. In performing this audit, we relied on electronic data files we obtained from Fresno, Los Angeles, Marin, and Sacramento. These files included reports from the agencies' ALPR systems. Because the agencies relied on remote third-party systems to produce the reports, our analysis of these reports was limited to verifying that we had received the information we requested. We did so by reviewing source materials such as user manuals, interviewing vendor staff, and confirming with the agency staff that the number of records in the files we received were correct. We also used electronic lists from the California Police Chiefs Association and the California State Sheriffs' Association to compile a list of statewide police and sheriff departments for our survey. We verified the nature of the data with the associations' staffs, and we also verified record counts by comparing the provided lists with FBI crime-reporting data. We found the data to be sufficiently reliable for our purposes.

Blank page inserted for reproduction purposes only.

XAVIER BECERRA
Attorney General

State of California
DEPARTMENT OF JUSTICE

1300 I STREET
SACRAMENTO, CA 95815-4524
Public: (916) 210-5000
Fax (916) 227-3079
Email: Joe.Dominic@doj.ca.gov

January 28, 2020

Elaine Howle
California State Auditor
621 Capitol Mall, Suite 1200
Sacramento, CA 95814

Re: Draft Audit Report - California State Auditor Report 2019-118; Automated License Plate Readers (ALPR)

Dear Ms. Howle:

The Department of Justice (DOJ) appreciates the opportunity to review the above-mentioned draft audit report. DOJ currently has no program in place to provide policy template and guidance to law enforcement agencies for their ALPR programs. Express authority from the Legislature and funding are needed to implement the recommendations.

If you have any questions or concerns regarding this matter, you may contact me at the telephone number listed above.

Sincerely,

Joe Dominic, Chief
California Justice Information Services Division

For XAVIER BECERRA
Attorney General

cc: Sean McCluskie, Chief Deputy to the Attorney General
Edward Medrano, Chief, Division of Law Enforcement
Chris Prasad, CPA, Director, Office of Program Oversight and Accountability

Blank page inserted for reproduction purposes only.

City of FRESNO
POLICE DEPARTMENT

ANDREW J. HALL
Chief of Police

Mariposa Mall
P.O. Box 1271
Fresno, CA 93715-1271

January 27, 2020

Elaine Howle
California State Auditor
621 Capitol Mall, Suite 1200
Sacramento, CA 95814

Dear Ms. Howle:

On behalf of the men and women of the Fresno Police Department, allow me the opportunity to thank you and your team for the time and effort in completing the Automated License Plate Reader (ALPR) audit at the request of the Joint Legislative Audit Committee. The Fresno Police Department always strives to ensure we maintain excellence and utilize best practices in all facets of service to the community especially concerning personal privacy. Building trust in the community is paramount to our agency as we continue our on-going efforts to be a model community policing agency. We will utilize this audit to ensure those goals are achieved.

The following are the Fresno Police Department's response to the audit recommendations included in the report.

1. *"To ensure that agency ALPR policies contain all of the required elements as specified in state law, by August 2020 Fresno should review their ALPR policies and draft or revise them as necessary. Also by August 2020 post their revised policies on their websites in accordance with state law:*

   The Fresno Police Department has already began reviewing and updating our ALPR policy. In fact, it is nearly complete and will be completed well in advance of the August 2020 recommended timeline.

2. *"To protect ALPR data to the appropriate standard, Fresno should do the following:"*
   a. *By August 2020 identify the types of data in their ALPR systems, and as they review or draft their policies, ensure that they clarify the types of information their officers may upload into their ALPR systems such as, but not limited to information obtained through CLETS."*

   As the audit showed, the Fresno Police Department has not entered personal data into the ALPR system; however we will continue to review data and incorporate into policy the parameters for types of data which can be entered.

   b. *By April 2020 perform an assessment of their ALPR systems data security features, and make adjustments to their system configurations where necessary to comply with CJIS policy best practices based on that assessment.*

The Fresno Police Department IT Manager will assess the ALPR system and ensure it is in compliance with CJIS Security Policy best practices.

3. *"To ensure that the agreement with their cloud vendor offers the strongest possible data protections, by August 2020 Fresno should enter into new contracts with Vigilant that contain the contract provisions recommended in CJIS policy."*

The Fresno Police Department IT Manager will review the Vigilant contract and ensure the contract is updated and in compliance with CJIS Security policy.

4. *To ensure that ALPR images are being shared appropriately:*
    a. *By April 2020 Fresno should review the entities with which they currently share images, determine the appropriateness of this sharing, and take all necessary steps to suspend those sharing relationships deemed inappropriate or unnecessary.*

The Fresno Police Department has suspended most sharing and now only shares images with bordering states.

    b. *By August 2020 Fresno should revise its written procedures for ALPR image sharing, as necessary, to ensure that it follows these procedures.*

The Fresno Police Department will incorporate these changes into the updated policy.

5. To minimize the privacy risk of retaining ALPR images for long periods of time, Fresno should do the following:
    a. *By August 2020 review the age of the ALPR images their personnel are searching for and ensure their retention periods for ALPR images are based on department needs. {REDACTED} reflect in its ALPR policy the updated retention period in its policy the updated retention period and state in its policy that it will reevaluate its retention period at least every two years.*

Based on the results of the audit, the Fresno Police Department will amend our current practice of retaining images for one year to six months which is consistent with the time frame the majority of the searches occur.

    b. *Include in their ALPR policies a retention period for data or lists such as hot lists, used to link persons of interest with license plate images, and create necessary processes to ensure that those data unrelated to ongoing investigations are periodically removed from their ALPR systems.*

The Fresno Police Department will maintain active hot lists for 90 days. If an investigator requires a longer period, approval will be obtained from a commander. This will be incorporated in the revised ALPR policy.

6. To enable monitoring of user access and user queries of ALPR images, Fresno should do the following:
    a. *By April 2020 assess the information their ALPR systems capture when users access them to ensure that the systems' logs are complete and accurate and that they form a reasonable basis for conducting necessary, periodic audits.*

    This is already being done and is part of the quarterly audit process.

    b. *Ensure their ALPR policies make clear how frequently they will audit their ALPR systems, who will perform those audits, who will review and approve the audit results, and how long they will retain the audit documents. [REDACTED] have in place by February 2021 an audit plan that describes its audit methodology, including, but not limited to, risk areas that will be audited, sampling, documentation, and resolution of findings.*

    A quarterly audit process has been put in place. The audit process, methodology and responsibilities will be included in the updated ALPR policy.

    c. *By June 2021 implement their audit plans and complete their first audits.*

    The audit process is already in place and audits were completed for the last two quarters of 2019.

7. To ensure that ALPR access is limited to agency staff who have a right and a need to use ALPR data, Fresno [REDACTED] should do the following:
    a. *By April 2020 review all user accounts and deactivate accounts for separated employees, inactive users, and others as necessary.*

    This has been completed. Separated employees are removed upon notification of their separation. The ALPR system automatically deactivates accounts for users who have been inactive for 365 days.

    b. *Ensure that their ALPR policies specify the staff classifications, ranks, or other designations that may hold ALPR system user accounts and that accounts are granted based on need to know and right to know.*

    This will be incorporated into the revised ALPR Policy. Access will be granted on a need to know and right to know basis for sworn department members and crime specialists who have investigative responsibility.

    c. *By August 2020 develop and implement procedures for granting and managing user accounts that include, but are not limited to, requiring that a supervisor must approve an account for a user, providing training to users before granting an account, suspending users after defined periods of inactivity, and requiring regular refresher training for active users and training for users before reactivating previously*

inactive accounts. [REDACTED] ensure that it has procedures in place to deactivate accounts immediately for account holders who separate from the agency or who no longer need a user account.

The Fresno Police Department will incorporate supervisor approval for new accounts and minimum training requirements for new users in the revised policy.

Sincerely,

Andrew J. Hall, Chief of Police
Fresno Police Department

AJH: rb

LOS ANGELES POLICE DEPARTMENT

MICHEL MOORE
Chief of Police

ERIC GARCETTI
Mayor

P. O. Box 30158
Los Angeles, Calif. 90030
Telephone: (213) 486-0150
TDD: (877) 275-5273
Ref #: 1.1

February 4, 2020

Elaine Howle*
California State Auditor
621 Capitol Mall, Suite 1200
Sacramento, CA 95814

Dear Ms. Howle:

In response to your draft report titled "Automated License Plate Readers: To Better Protect Individuals' Privacy, Law Enforcement Must Increase Its Safeguards Over the Data It Collects," I would like to inform you that the Los Angeles Police Department (LAPD) has the utmost respect for individuals' privacy and currently has policies and procedures in place to safeguard personal information stored on the Automated License Plate Reader (ALPR) Systems. Personnel who utilize ALPR data have been through extensive training on accessing and using the data on a right to know and need to know basis. The LAPD continuously reviews all user accounts and deactivates accounts for separated employees, while allowing ALPR access to all active employees who have attended the training. ① ②

Although our dedication to protecting individuals' privacy is covered in our day to day operations and procedures, the Department is currently working on an ALPR policy to ensure that the protection of those rights is also memorialized in our Department Manual. The aforementioned ALPR policy will be completed by April 2020 and posted on the Department website once it is completed, as required by state law. The policy will address the types of information personnel may upload into the ALPR systems, as well as the retention period for the data or lists (i.e., hot lists used to link persons of interest with license plate images). The LAPD will perform an assessment of the systems' data security features and retention periods for ALPR images to evaluate the need for adjustment, prior to publishing of the ALPR policy. Furthermore, the policy will list the entities the Department shares ALPR images with and the process for handling image-sharing requests.

To ensure the ALPR policy is up to date and our ALPR systems are capturing proper information, the Department will perform periodic audits to assess the information the systems capture when accessed by the Department users. Per the recommendations listed in your audit draft report, the Department will have a plan that describes the periodic audits by February 2021 and will complete the first audit by June 2021.

Should you have any questions concerning this matter, please contact Sergeant Monica Tokoro, at (213) 486-0197.

Very truly yours,

MICHEL R. MOORE
Chief of Police

* California State Auditor's comments appear on page 61.

Blank page inserted for reproduction purposes only.

Comments

CALIFORNIA STATE AUDITOR'S COMMENTS ON THE RESPONSE FROM THE LOS ANGELES POLICE DEPARTMENT

To provide clarity and perspective, we are commenting on the response to our audit report from the Los Angeles Police Department. The numbers below correspond with the numbers we have placed in the margin of its response.

Los Angeles is the only one of four agencies we audited that did not have the ALPR policy state law requires. As we describe on page 15, state law requires law enforcement agencies to have written usage and privacy policies and for the policies to include various elements. As we describe on page 17, the program administrator for Los Angeles initially believed that the agency's many IT policies cover the ALPR program, but we identified deficiencies in the policies he shared with us. When we brought those deficiencies to the administrator's attention, he acknowledged the need for Los Angeles to have an ALPR policy. ①

We stand by our conclusion that Los Angeles does not follow best practices for granting users ALPR system access. As we describe on page 33, of the four agencies we reviewed Los Angeles was the most lax in its approach to authorizing user accounts. The protocol its IT division follows is to include its ALPR software on each computer it assigns to staff, regardless of their position. Thus, staff who do not perform functions related to the ALPR system and possibly have not had training, nevertheless have access to the system. Moreover, on page 34 we state that the detective who conducts ALPR training confirmed that Los Angeles has not required training before users can access the ALPR system. ②

Blank page inserted for reproduction purposes only.

COUNTY OF MARIN

OFFICE OF THE
COUNTY COUNSEL

Brian E. Washington
COUNTY COUNSEL

Jack F. Govi
ASSISTANT COUNTY COUNSEL

Renee Giacomini Brewer
CHIEF DEPUTY COUNTY COUNSEL

Patrick M. K. Richardson
Stephen R. Raab
Steven M. Perl
Brian C. Case
Jenna J. Brady
Valorie R. Boughey
Kerry L. Gerchow
Tarisha K. Bal
Deidre K. Smith
Brandon W. Halter
Sarah B. Anker

DEPUTIES

Colleen McGrath
ADMINISTRATIVE SERVICES OFFICER

Marin County Civic Center
3501 Civic Center Drive
Suite 275
San Rafael, CA 94903
415 473 6117 T
415 473 3796 F
415 473 2226 TTY
www.marincounty.org/cl

January 28, 2020

Elaine M. Howle, CPA*
California State Auditor
621 Capitol Mall, Suite 1200
Sacramento, CA 95814

Dear Ms. Howle:

The Marin County Sheriff's Office appreciates the opportunity to respond to your draft report entitled, Automated License Plate Readers: To Better Protect Individuals' Privacy, Law Enforcement Must Increase Its Safeguards Over the Data It Collects.

The Marin County Sheriff's Office is pleased to note that although your draft report includes recommendations to the Marin County Sheriff's Office regarding its use of automated license plate reader (ALPR) cameras, your audit team did not find any evidence of abuse or misuse of ALPR data by the Marin County Sheriff's Office. (1)

Nevertheless, the Marin County Sheriff's Office is and remains committed to the need for further improvement and as stated in your draft report, will consider your report's recommendations. However, based on some of the redactions in the draft report, it is difficult, at times, to determine which findings and conclusions are in reference to the Marin County Sheriff's Office as opposed to the other confidential law enforcement agencies discussed in your draft report. (2)

Accordingly, in responding to the issues discussed in your draft report with additional details and/or context, the Marin County Sheriff's Office will address sections which may not apply to it because it is unable to distinguish which law enforcement agency is being implicated. (2)

The following is the Marin County Sheriff's Office response:

Recommendation No. 1: Improve their ALPR polices.

Response to Recommendation No. 1: While the Marin County Sheriff's Office agrees that its current policy regarding the ALPR system does not specifically describe a "process for periodic system audits," the Marin County Sheriff's Office's policy does state that user/data query audits would be performed. Moreover, although the audit team contends that the ALPR data collected by the

* California State Auditor's comments begin on page 67.

PG. 2 OF 4

Marin County Sheriff's Office qualifies as personal information, this is not the case. The draft report readily admits that there is no personally identifiable information contained in a license plate capture. Further, the audit team's erroneous belief is based on a free text box in the ALPR system wherein a user *could* enter a person's name in this text box and attach personal information to the images of license plates captured by the ALPR system. However, the Marin County Sheriff's Office does not utilize this free text box and does not enter any other personal information to be associated with the images taken by its ALPR system. In fact, the draft report concedes this fact as it states in regard to the Marin County Sheriff's Office and open text fields, the audit team "did not find personal information in combination with other sensitive information in the six months of search records [it] studied."

Recommendation No. 2: Implement needed ALPR data security.

Response to Recommendation No. 2: As noted in the draft report, the Marin County Sheriff's Office contracts with a third-party vendor Vigilant Solutions (Vigilant) regarding its ALPR system. While the audit team is critical of Vigilant, all access to Vigilant for the Marin County Sheriff's Office is activity logged and auditable as noted in the draft report, even if the user accesses the system via the internet with a personal device, and those logs are reviewed by the Marin County Sheriff's Office ALPR program administrator; all data on Vigilant is stored on secure servers in the United States as recommended by the audit team; and Vigilant only permits credentialed law enforcement officers with a valid Originating Agency Identifier (ORI) number issued by the Criminal Justice Information System (CJIS) Division of the Federal Bureau of Investigation (FBI). Additionally, as part of its services, Vigilant maintains it is compliant with all relevant requirements set forth in the FBI-CJIS Security Policy as recommended by the audit team.

Recommendation No. 3: Update vendor contracts with necessary data safeguards.

Response to Recommendation No. 3: As discussed above, while not explicitly stated in the Marin County Sheriff's Office's contract with Vigilant, Vigilant warrants in its services that the data captured by an agency remains the property of the agency; all data is stored on secure servers in the United States; and it conforms with all relevant requirements set forth in the FBI-CJIS Security Policy.

Recommendation No. 4: Ensure that sharing of ALPR images is done appropriately.

Response to Recommendation No. 4: As discussed above, the Marin County Sheriff's Office has confirmed with Vigilant that it has and continues to verify that it only permits credentialed law enforcement officers with a valid ORI number issued by the CJIS Division of the FBI access to the data on its hosted

server. While the audit team was critical of the Marin County Sheriff's Office sharing information with agencies such as the Honolulu Police Department, such cooperation with this particular law enforcement agency was done properly and with consideration as to the multiple matters which have in the past involved both agencies. (6)

As for ICE access, any prior approval by the Marin County Sheriff's Office with Vigilant was before any of the relevant state law went into effect. As noted in the draft report, Vigilant confirmed that the recent viewing of ICE accounts in question were not active and that these inactive agencies were not previously visible to the Marin County Sheriff's Office. (6)

Recommendation No. 5: Evaluate and reestablish data retention policies.

Response to Recommendation No. 5: The Marin County Sheriff's Office's two-year retention policy is based on the statute of limitations for most crimes in the State of California. The audit team states that it would like the Marin County's Sheriff's Office to have a more detailed policy regarding retention based on usefulness of images to investigators and even suggest that the retention of the images should be based on whether the images are for minor crimes versus complex crimes. However, it would be impossible for the Marin County Sheriff's Office to know whether the captured images would be used in a minor criminal case or a major felony case at the time the images were taken or at any time afterwards. Indeed, as noted in the draft report, there is no statute of limitations for the crime of murder. (7)

Recommendation No. 6: Develop and implement procedures for granting and managing user accounts.

Response to Recommendation No. 6: The audit team believes that the Marin County Sheriff's Office should require supervisory approval for all users of its ALPR system. As noted above and in the draft report, at this time the Marin County Sheriff's Office does not believe that this particular requirement is appropriate for the following reasons: there is no personal information associated with the images taken by the Marin County Sheriff's Office; as discussed in the draft report, all users of the ALPR system receive training before they are permitted access to the ALPR system; and the Marin County Sheriff's Office regularly audits the use of the ALPR system. (8)

Recommendation No. 7: Develop and implement ALPR system oversight.

Response to Recommendation No. 7: In the draft report, the audit team identifies an incident in which it claims it brought to the Marin County Sheriff's Office's attention an active account for a resigned employee. However, this is not accurate. The system administrator was notified about deactivating the account on the same day the audit team informed him about this account. However, the (9)

ALPR administrator had deactivated the account *prior* to the audit team discussing this particular account with him. Moreover, the ALPR administrator does not solely rely on a department-wide email notification regarding resigned or terminated employees as discussed in the draft report. In addition to the audits he regularly performs, the ALPR administrator also performs periodic spot checks to verify that active accounts match active employees.

Should you have any questions regarding this response, including any comments and clarifications made herein, please do not hesitate to contact us directly.

Sincerely,

Kerry L. Gerchow
Deputy County Counsel

Comments

CALIFORNIA STATE AUDITOR'S COMMENTS ON THE RESPONSE FROM THE MARIN COUNTY SHERIFF'S OFFICE

To provide clarity and perspective, we are commenting on the response to our audit report from the Marin County Sheriff's Office. The numbers below correspond with the numbers we have placed in the margin of its response.

Marin's response correctly notes that our review of its internal affairs investigations records did not identify evidence of abuse or misuse of ALPR data. However, as we state on page 37, we do not consider this absence as proof that no instances of ALPR misuse occurred. There is the possibility that misuse occurred and went unnoticed and unreported, particularly since Marin does not conduct audits of its ALPR system. (1)

During our exit conference, we specifically informed Marin that we would send it only those portions of the draft report that were relevant to it. The text that we redacted pertains to the other entities that were part of the audit and that we are required by law to keep confidential. Further, during its review of the draft report, Marin did not communicate with us to seek clarification regarding the report content we provided, despite our providing multiple opportunities for it to do so. (2)

Marin is incorrect in stating that we contend that the license plate images Marin collects qualify as personal information. On page 11, we note that a law enforcement agency can enter additional information, such as personal information, into its ALPR system. However, we do not assert that the ALPR image alone contains personal information. (3)

Marin has mischaracterized our finding. In its response, Marin states that we based our conclusion on a free-text box wherein a user could enter an individual's name and attach it to a license plate image. However, as we describe on pages 18 and 19, we based our conclusion on information that users enter into open text fields as part of license plate searches, specifically the fields for case numbers and purpose for the searches. On page 37, we note that Marin requires users to enter both case numbers and reasons for the search before allowing such searches. Although we did not find evidence users had entered personal information in combination with other sensitive information in the six months of search records we studied, the fact that these text fields exist means that users could enter such information during ALPR searches, as we point out on pages 18 and 19. Moreover, Marin's ALPR policy does not prohibit users from entering personal information in combination with other sensitive information in its ALPR system. (4)

⑤ We disagree with the focus of Marin's response, which implies that the vendor's security controls are a suitable substitute for specific contract safeguards. As we show in Figure 3 on page 22, Marin's contract does not contain any of the safeguards CJIS policy recommends for contracts with cloud vendors. We note on page 21 that CJIS policy states that ambiguous contract terms can lead to controversy over data privacy and ownership rights, whereas a contract that clearly establishes data ownership acts as a foundation for trust that the cloud vendor will protect the privacy of the agency's data.

⑥ We disagree with Marin's belief that it has managed its image sharing appropriately. Although Marin described in its response the type of information that it could maintain to document its image-sharing decisions, it did not provide such evidence documenting why it made past sharing decisions, and its ALPR policy does not include a process for approving image-sharing requests, as we state on page 26. Moreover, Marin acknowledged in its response the issue we describe on page 26 regarding ICE and the fact that the status of Marin's sharing relationship with ICE was not always visible to Marin. This issue underscores the need for Marin to maintain records regarding sharing decisions.

⑦ Marin appears to miss the point of our recommendation. As we state on page 29, we concluded that Marin did not establish its retention period based on when it uses the ALPR images it captures. On page 31, we mention minor and complex crimes as examples of ALPR data being used narrowly, such as for the single purpose of locating stolen vehicles, or broadly, such as for investigation of crimes in addition to stolen vehicles. Our recommendation—based on our analysis of Marin's search activity as referenced on page 30—provides a method for Marin to better align how long it retains ALPR data with whether it actually uses the data as they age.

⑧ The reasons Marin cites in its response for not adopting our recommendation are not valid. Requiring a supervisor to approve a user for an ALPR account is a meaningful step in establishing that user's need to access ALPR data and right to know what the data portray in an effort to avoid the ALPR data being misused. In point 4 above, we describe that the existence of text fields in the ALPR system allows for personal information to be linked to license plate images. Further, we note that Marin has no policy prohibiting its users from entering personal information in its ALPR system. In addition, despite Marin's claim of training all users, we state on page 34 that Marin does not require staff to renew their training when reactivating their user accounts following long periods of not using the ALPR system. Finally, we found that contrary to Marin's assertion, it had not regularly audited its system. As we discuss

on page 37, Marin's ALPR administrator was unaware of the state law requiring audits of ALPR systems, so he had not been conducting them. Despite recent efforts to institute some form of monitoring, as we describe on page 38, the limitations in its approach led us to conclude that Marin does not have sufficient protocols in place to detect the misuse of user accounts.

Marin's assertion is incorrect. As we describe on page 35, we reviewed Marin's processes for disabling the accounts of separated employees. Although Marin's ALPR administrator informed us of his approach for deactivating an account when he receives an all-staff email that an employee is separating from the department, we found such an email dated August 6, 2019, after which one separated employee continued to hold an active account as of October 22, 2019. After we informed the administrator of this employee's continued access, the administrator acknowledged that the account was still active, and we directly observed him deactivating the account. ⑨

Blank page inserted for reproduction purposes only.

Human Assistance
Ann Edwards, Director

County of Sacramento

Branches
Customer Service Operations
Finance and Administration
Community and Program Support

County Veterans Services Office

January 27, 2020

Elaine M. Howle
California State Auditor
621 Capitol Mall, Suite 1200
Sacramento, CA 95814

SUBJECT: License Plate Readers Audit Response

Dear Ms. Howle:

We are writing in response to the draft findings of your report, titled Automated License Plate Readers: To Better Protect Individuals' Privacy, Law Enforcement Must Increase Its Safeguards Over the Data It Collects.

The Department of Human Assistance (DHA) appreciates the work performed by the California State Auditor. No recommendations were issued in the report, and DHA agrees with the results of the audit.

If you have any questions regarding this matter, please contact Lane Ruddick, Program Integrity Chief, by telephone at (916) 875-1275, or by email at ruddickl@saccounty.net.

Sincerely,

Ann Edwards
Director

Blank page inserted for reproduction purposes only.

SACRAMENTO COUNTY SHERIFF'S OFFICE

Scott R. Jones
Sheriff

January 28, 2020

Elaine M. Howle, CPA*
California State Auditor
621 Capitol Mall, Suite 1200
Sacramento, CA 95814

Dear Ms. Howle:

I am in receipt of the draft report entitled *Automated License Plate Readers: To Better Protect Individuals' Privacy, Law Enforcement Must Increase Its Safeguards Over the Data It Collects, which* includes recommendations for the Sacramento County Sheriff's Office to revise and improve some of our Automated License Plate Reader program (ALPR) processes.

While I agree with some of your findings, I disagree with some of the characterizations made. ① As the Sheriff of Sacramento County, I take seriously the protection of our citizens, including their personal privacy. Within our role as guardians of the data we collect, my staff works diligently to develop and consistently apply security protocols that maintain the integrity of our systems.

The Summary (Results in Brief) section of the report was clearly written separately or prior to ① the completion of the main body of the report, because it fails to present your teams' actual conclusions. Let me address each point.

Recommendation #1 – Review and revise policies

Before the Audit began, the Sacramento County Sheriff's Office began reviewing and revising policies governing a wide range of service deliverables. Although the Sacramento County Sheriff's Office existing policy contains the majority of the requirements outlined in California Civil Code section 1798.90.51, it does not list the restriction on selling ALPR data. As expressed during the interviews, my staff did say that the restriction on selling data is not listed in the policy because the Sacramento Sheriff's Office does not sell any data. The lack of specifically addressing this fact in the ALPR policy is an oversight.

* California State Auditor's comments begin on page 77.

Elaine M. Howle, CPA
January 28, 2020
Page 2

Recommendation #2 – Identify types of data and perform a security assessment

As you learned during the audit, the Sacramento County Sheriff's Office began reorganizing ALPR related security over two years ago. The initial step of this process was securing funding to hire a fulltime Information Technology Analyst in hopes of increasing program administration because this employee's primary job will be the continuous development of ALPR related security protocols that either meet or exceed these recommendations.

Recommendation #3 – Ensure the vendor offers the strongest possible data protections

The Sacramento County Sheriff's Office completed extensive research in the use of cloud storage systems and CJIS security. I am aware your team received the latest contract between the Sacramento County Sheriff's Office and Vigilant Solutions and the Vigilant CJIS Security Policy Guide. Both the contract and comprehensive policy provide a thorough explanation regarding compliance including agreeing to participate in any Technical Security Compliance Audit performed by the FBI-CJIS Division. (2)

Recommendation #4 – Develop a process for handling ALPR image-sharing requests

(3) Although the existing policy does provide language on how sharing data can occur, the Sacramento County Sheriff's Office began developing a ticketing system for handling various technology requests over four years ago. As such, the natural progression was to utilize the same request, approval, and record retention system used by the entire organization.

Recommendation #5 – Review the retention periods of ALPR images and data

The Sacramento County Sheriff's Office is continually reviewing data retention practices. Although, a simple review of searches provides a small subset of activity, the success of an ALPR program could only come from tracking and identifying which cases provided leads or convictions of data. (4) During the audit, my understanding is your team was told this very fact. As the agency prepares to transition to a new report writing system, I request our crime analysts to conduct a multi-year study that will provide a realistic view of how long ALPR images provide usefulness in the criminal justice system.

Recommendation #6 – Enable monitoring of user access and user queries of ALPR images

Throughout the audit your team requested a substantial number of reports and logs showing when accounts were activated, deactivated, or changes occurred. The ability to provide these reports demonstrated the robust nature of the logging system. Although your team learned the

Sacramento County Sheriff's Office has no reported incidents of ALPR misuse, I have directed my program administrator to make certain fields mandatory to ensure proper documentation of usage. With the addition of a dedicated IT Analyst, the expansion of audits already occurring will surely continue.

Recommendation #7 – Ensure that ALPR access is limited to agency staff who have a right and a need to know

Not only is this recommendation listed in the Sacramento County Sheriff's Office policy, it is the way the organization operates with all data systems. As this directly relates to ALPR, only 561 employees, out of a department of 2,170, have access to the system. While I understand your position that a supervisor should approve each account, there were over 5,880 personnel moves during 2019. The Sacramento County Sheriff's Office uses Role Based Access Controls. Rather than rely solely on a supervisor to approve a request, the application of Role Based Access Control is how the Security Operations unit of the Sacramento Sheriff's Office processes access to this and all other law enforcement data systems. Role Based Access Controls are addressed by the National Institute of Standards and Technology as a best practice. (5)

In Conclusion

In the end, we are not opposed to implementing many of your recommendations and in fact, are already in the process of doing so. Throughout the process, which was long and took many staff hours, we made every effort to cooperate with the auditor's requests for information and tried to anticipate the types of problems they would find while trying to understand the actual uses and practices within the ALPR program.

During interviews and based on some of the requests, we felt concern that there was a bias toward a particular outcome, intended or otherwise. (6) Because this report contains many redacted sections, there is still some concern about what has not been shown to us. Nonetheless, we await your full findings about Sacramento and the other agencies covered in this report. (7)

Very truly yours,

Scott Jones

SCOTT R. JONES, SHERIFF

Blank page inserted for reproduction purposes only.

Comments

CALIFORNIA STATE AUDITOR'S COMMENTS ON THE RESPONSE FROM THE SACRAMENTO COUNTY SHERIFF'S OFFICE

To provide clarity and perspective, we are commenting on the response to our audit report from the Sacramento County Sheriff's Office. The numbers below correspond with the numbers we have placed in the margin of its response.

We stand by the language we use to describe Sacramento's ALPR program. Our report provides appropriate context and sufficient evidence to support our findings. Further, the Results in Brief section of the report serves as a summary of the report as a whole and as such it represents the overall conclusions for this report. The details of our findings and conclusions are included in the Audit Results section of the report. ①

We disagree with Sacramento's contention that the department's current contract is thorough. On pages 22 and 23, we acknowledge that Sacramento updated its contract with Vigilant in September 2019. In reviewing that latest version, we determined that it is missing some of the best practices outlined in CJIS policy, as we show in Figure 3 on page 22. On page 21, we note that CJIS policy states that a contract that clearly establishes data ownership acts as a foundation for trust that the cloud vendor will protect the privacy of the agency's data. ②

Sacramento's response implies that a process for approving image-sharing requests and maintaining records outside of the Vigilant system was already in place. However, although Sacramento states that it began developing a ticketing system for handling technology requests more than four years ago, as we discuss on page 26, Sacramento could not provide any evidence of records outside of the Vigilant user interface demonstrating when or why it agreed to share with particular entities. As we further point out on page 26, Sacramento's ALPR policy currently does not include a process for approving sharing requests. ③

Sacramento's proposed study of ALPR images may benefit its ALPR program. Our analysis of the search records from the agencies we reviewed—summarized on page 30 and in Table 2—presents one method of identifying the age of the data personnel are using. We point out on page 31 that the agencies' existing ALPR systems provide the ability to conduct such an analysis. Nevertheless, our recommendation does not preclude the type of analysis Sacramento describes in its response. ④

⑤ We stand by our recommendation that Sacramento should have a policy that clearly states the staff classifications, ranks, or other designations that may hold ALPR system user accounts and that accounts are granted based on a need to know and a right to know. As we state on page 32, each ALPR administrator, including Sacramento's, stressed the concept of "need to know, right to know." Assigning an individual an ALPR account based strictly on his or her classification or role—the practice Sacramento follows—does not ensure that an individual has a need to know because of their specific assigned work.

⑥ Sacramento's concern about bias is unfounded. To meet generally accepted government auditing standards, which my office is obligated to comply with, we have and follow policies and procedures for all audits to ensure that we identify and rectify any threats to our independence, including bias. Moreover, we follow quality control procedures on every audit that ensure that we have sufficient and appropriate evidence to support our findings and conclusions.

⑦ Sacramento received draft text that was relevant to our findings about it. State law requires us to keep confidential information about an unpublished audit. Consequently, we cannot share with one agency information about another. Sacramento received a draft audit report with redacted information regarding other agencies as necessary to maintain confidentiality. During our exit conference, we stressed that staff should contact us with questions they might have about the draft report during the formal review period; Sacramento did not contact us. We also contacted Sacramento's ALPR administrator during the formal review period to inquire about questions staff may have, and he did not return our call.

EXHIBIT H

California Department of Justice DIVISION OF LAW ENFORCEMENT John D. Marsh, Chief		**INFORMATION BULLETIN**	
Subject: **California Automated License Plate Reader Data Guidance**		*No.* 2023-DLE-06 *Date:* 10/27/2023	*Contact for information:* John D. Marsh, Chief Division of Law Enforcement (916) 210-6300

TO: ALL CALIFORNIA STATE AND LOCAL LAW ENFORCEMENT AGENCIES

This Information Bulletin provides guidance to California state and local law enforcement agencies (collectively California LEAs) regarding the governance of Automated License Plate Recognition (ALPR) information to ensure that the storage, collection, sharing, and use of this information is consistent with California law.

According to a recent survey and report issued by the California State Auditor[1], the majority of California LEAs collect and use images captured by ALPR cameras. While ALPR information may be a helpful tool for investigative purposes, California law governs the collection, storage, sharing, and use of this data. In particular, Senate Bill 34 (Statutes of 2015, Chapter 532) (SB 34) imposes requirements on ALPR system operators and end-users regarding ALPR data collected through an ALPR system, including with whom this information may be shared.

This Information Bulletin should serve as a reminder and a resource for California LEAs to ensure that their collection, storage, sharing, and use of ALPR information complies with California law.

State Law Governing Use of Automated License Plate Reader Data (SB 34)

Senate Bill 34 (Statutes of 2015, Chapter 532) (SB 34) became effective on January 1, 2016. That law, codified at California Civil Code section 1798.90.5 *et seq*., establishes requirements—including privacy safeguards— for California LEAs who collect, store, use, or share ALPR data. Additional requirements apply to agencies that operate an ALPR system. Key definitions from SB 34 are set forth below:

- *"*ALPR information*"* is "information or data collected through the use of an ALPR system [excluding a transportation agency]." (Civ. Code, § 1798.90.5, subd. (b).)

- "ALPR system" means "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 of registration plates and the characters they contain into computer-readable data." (Civ. Code, § 1798.90.5, subd. (d.)

- "ALPR operator*"* is "a person that operates an ALPR system, but does not include a transportation

[1] The full report is available at https://www.auditor.ca.gov/reports/2019-118/index.html

agency when subject to Section 31490 of the Streets and Highways Code.].) (Civ. Code, § 1798.90.5, subd. (c)

- An "ALPR end-user" is "a person that accesses or uses an ALPR system," with exclusions not relevant to LEAs. (Civ. Code, § 1798.90.5, subd. (a).)

- A "person" is "any natural person, public agency, partnership, firm, association, corporation, limited liability company, or other legal entity." (Civ. Code, § 1798.90.5, subd. (e).)

- A "public agency" is "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." (Civ. Code, § 1798.90.5, subd. (f).)

GUIDANCE REGARDING SB 34

As a reminder, SB 34 imposes the following affirmative obligations on "public agencies," which includes all California LEAs:

- A public agency "shall not sell, share, or transfer ALPR information, except to another public agency, and only as otherwise permitted by law." "[T]he provision of data hosting or towing services shall not be considered the sale, sharing, or transferring of ALPR information." (Civ. Code, § 1798.90.55, subd. (b).)

- A public agency that operates or intends to operate an ALPR system must provide the opportunity for public comment at a regularly scheduled meeting of the agency before implementing the ALPR program. (Civ. Code, § 1798.90.55, subd. (a).)

- ALPR operators and end-users must develop a usage and privacy policy, which must be conspicuously posted on their website, and must contain provisions designed to "protect ALPR information from unauthorized access, destruction, use, modification, or disclosure." (Civ. Code, §§ 1798.90.53, subds. (a)-(b); 1798.90.51, subd. (a)-(b);)

Agencies should carefully examine their policies and procedures to determine whether they are an ALPR operator and/or end-user, as defined above, and whether they have complied with the obligations of operators and end-users as set forth in SB 34.

Prohibition on the Sale, Sharing, or Transfer of ALPR Information

Regardless of whether an LEA is an ALPR operator or ALPR end-user, SB 34 prohibits any public agency from selling, sharing, or transferring ALPR information "except to another public agency, and only as otherwise permitted by law." (Civ. Code, § 1798.90.55, subd. (b).) Data hosting or towing services are not considered the sale, sharing, or transferring of ALPR information. (*Ibid.*)

Importantly, the definition of "public agency" is limited to state or local agencies, including law enforcement agencies, and does not include out-of-state or federal law enforcement agencies. (See Civ.

Code, § 1798.90.5, subd. (f).) Accordingly, SB 34 does not permit California LEAs to share ALPR information with private entities or out-of-state or federal agencies, including out-of-state and federal law enforcement agencies. This prohibition applies to ALPR database(s) that LEAs access through private or public vendors who maintain ALPR information collected from multiple databases and/or public agencies.

California LEAs are encouraged to review their data user agreements to ensure that they comply with SB 34 and do not allow access to agencies other than state and local agencies, or permitted private entities for purposes of data hosting or towing services.

In responding to a Public Records Act request or compulsory process in litigation seeking the production of ALPR information, California LEAs should consider all applicable privileges and exemptions depending on the nature of the request, bearing in mind the command in Civil Code section 1798.90.55, subdivision (b), that an ALPR end-user or operator "shall not sell, share, or transfer ALPR information, except to another public agency, and only as otherwise permitted by law."

Guidance for California LEA ALPR Operators

California LEAs that ***operate*** an ALPR system are encouraged to ensure they are in compliance with the following SB 34 requirements:

- Maintain reasonable security procedures and practices to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure. (Civ. Code, § 1798.90.51, subd. (a).)

- Implement a usage and privacy policy, which must be available to the public in writing and posted conspicuously on the LEA's internet website.

    - SB 34 contains numerous requirements regarding the content of this policy. (See Civ. Code, § 1798.90.51, subd. (b).) Please see the attached template policy that the California Department of Justice has drafted to assist California LEAs that are operators and/or end-users in complying with SB 34.

- Do the following, if the ALPR operator accesses or provides access to ALPR information (for example, to other LEAs by permitting access to its ALPR database):

    - Maintain a record of that access, including:

        - The date and time the information is accessed;

        - The license plate number or other data elements used to query the ALPR system;

        - The user name of the person who accesses the information and, if applicable, the organization or entity with whom the person is affiliated; and

        - The purpose for accessing the information. (Civ. Code, § 1798.90.52, subd. (a).)

    - Require that ALPR information only be used for the authorized purposes described in its ALPR privacy policy. (Civ. Code, § 1798.90.52, subd. (b).)

- Comply with the requirement to "provide an opportunity for public comment at a regularly scheduled public meeting of the governing body of the public agency before implementing the program." (Civ. Code, § 1798.90.55, subd. (a).)
    - This means that agencies that have not yet implemented an ALPR program but are contemplating doing so must provide an opportunity for public comment regarding the proposed program at a regularly scheduled meeting of the agency's governing body before implementing the program.
    - Although the law does not address ALPR programs that were implemented before January 1, 2016 (when SB 34 was enacted), in keeping with the purpose of SB 34, agencies whose programs predate SB 34, LEAs should consider providing an opportunity for public comment on its ALPR program at a regularly scheduled public meeting of the agency's governing body.
    - Agencies that implemented an ALPR program after January 1, 2016, without providing an opportunity for public comment, should likewise consider providing such an opportunity at a regularly scheduled meeting of the agency's governing body.

Guidance for California LEA ALPR End-Users

LEAs that **access or use** an ALPR system (which, as defined above, includes a searchable computerized database with information obtained from ALPR cameras) should ensure they are in compliance with the following SB 34 requirements:

- Maintain reasonable security procedures and practices to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure. (Civ. Code, § 1798.90.53, subd. (a).)

- Implement a usage and privacy policy, which shall be available to the public in writing and posted conspicuously on the agency's website. (Civ. Code, § 1798.90.53, subd. (b)(1).)

    - SB 34 contains numerous requirements regarding the content of this policy. (See Civ. Code, § 1798.90.53, subd. (b)(2).) Please see the attached template policy that the California Department of Justice has drafted to assist California LEAs that are operators and/or end-users in complying with SB 34.

As a reminder, SB 34 requires California LEAs that operate as either ALPR operators and/or end-users to conspicuously display their ALPR policies on their agency's website, if they have a website. Inclusion of such a policy in a manual, without noting on the main web page of their agency the existence of and/or link to such a policy, may not satisfy SB 34's requirement that such policies be "posted conspicuously on that Internet Web site." (Civ. Code, §§ 1798.90.51, subs. (b)(1), 1798,90.53, subd. (b)(1).)

Accessing the FBI's National Crime Information Center (NCIC) and CA DOJ License Plate Data

In addition to the requirements in this bulletin related to ALPR data, LEAs may access NCIC and California Department of Justice license plate data files, to be used for law enforcement purposes only, subject to the authorization process and restrictions summarized in Bulletin #23-01-CJIS [Updated California Value's Act's Database Guidance].

Additional Reference Materials

Going forward, as your agency utilizes ALPR technology and related file downloads, you are encouraged to regularly review your policies and usage to help ensure all applicable requirements are being adhered to. As additional reference materials, the following resources are included for your consideration as well:

- **California State Auditor's Report, 2019-118**
  "ALPRS: To Better Protect Individuals' Privacy, Law Enforcement Must Increase Its Safeguards for the Data it Collects"
  https://www.auditor.ca.gov/reports/2019-118/index.html

- **DOJ Information Bulletin, 18-10-CJIS**
  "California Values Act's Database Guidance"
  https://oag.ca.gov/sites/all/files/agweb/pdfs/info_bulletins/18-10-cjis.pdf

- **DOJ Information Bulletin, 23-01-CJIS**
  "Updated California Value's Act's Database Guidance"
  https://oag.ca.gov/info-bulletins

For questions about this Information Bulletin, please contact Division of Law Enforcement Chief John Marsh at (916) 210-6300.