Date of Hearing: April 22, 2021

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 1076 (Kiley) – As Introduced February 18, 2021

SUBJECT: Automated license plate recognition systems: model policy

SUMMARY: This bill would require the Department of Justice (DOJ) to draft and make available on its internet website an automated license plate recognition system (ALPR) policy template for local law enforcement agencies, and additionally require the DOJ to develop and issue guidance for local law enforcement agencies to help them identify and evaluate the types of data they are storing in their systems.

EXISTING LAW:

1) Provides, pursuant to the California Constitution, that all people have inalienable rights, including the right to pursue and obtain privacy. (Cal. Const., art. I, sec. 1.)

2) Defines "automated license plate recognition system" or "ALPR system" to mean 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. "ALPR information" means information or data collected through the use of an ALPR system. "ALPR operator" means a person that operates an ALPR system, except as specified. "ALPR end-user" means a person that accesses or uses an ALPR system, except as specified. The definitions for both ALPR operator and ALPR end-user exclude transportation agencies when subject to Section 31490 of the Streets and Highways Code. (Civ. Code Sec. 1798.90.5.)

3) Requires an ALPR operator 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. ALPR operators must implement usage and privacy policies 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. It further requires the policies to include, at a minimum, certain elements. (Civ. Code Sec. 1798.90.51.)

4) Requires ALPR end-users to maintain reasonable security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect ALPR information from unauthorized access, destruction, modification, or disclosure. ALPR end-users must implement usage and privacy policies in order to ensure that the access, use, sharing, and dissemination of ALPR information is consistent with respect for individuals' privacy and civil liberties. It further requires the policies to include, at a minimum, certain elements. (Civ. Code Sec. 1798.90.53.)

5) Provides that 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. (Civ. Code Sec. 1798.90.55.)

6) Authorizes the Department of the California Highway Patrol (CHP) to retain license plate data captured by a license plate reader for no more than 60 days, except in circumstances when the data is being used as evidence or for all felonies being investigated, including, but not limited to, auto theft, homicides, kidnaping, burglaries, elder and juvenile abductions, Amber Alerts, and Blue Alerts. (Veh. Code Sec. 2413(b).)

7) Prohibits CHP from selling license plate reader data for any purpose and from making the data available to an agency that is not a law enforcement agency or an individual who is not a law enforcement officer. The data may be used by a law enforcement agency only for purposes of locating vehicles or persons when either are reasonably suspected of being involved in the commission of a public offense. (Veh. Code § 2413(c).)

8) Requires CHP to monitor internal use of the license plate reader data to prevent unauthorized use. (Veh. Code Sec. 2413(d).)

9) Requires CHP to annually report the license plate reader practices and usage, including the number of license plate reader data disclosures, a record of the agencies to which data was disclosed and for what purpose, and any changes in policy that affect privacy concerns to the Legislature. (Veh. Code Sec. 2413(e).)

10) Establishes the data breach notification law, which requires any agency, person, or business that owns, licenses, or maintains data including personal information to disclose a breach, as provided. (Civ. Code Secs. 1798.29(a), (b), (c) and 1798.82(a), (b), (c).) Includes within the definition of "personal information," ALPR data when combined with an individual's first name or first initial and last name when either piece of data is not encrypted. (Civ. Code Secs. 1798.29(g), 1798.82(h).)

11) Prohibits a transportation agency from selling or otherwise providing to any other person or entity personally identifiable information of any person who subscribes to an electronic toll or electronic transit fare collection system or who uses a toll bridge, toll lane, or toll highway that employs an electronic toll collection system, except as expressly provided. (Sts. & Hy. Code Sec. 31490.)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Purpose of the bill**: This bill seeks to ensure that law enforcement agencies have access to model policies that provide adequate safeguards for their ALPR data. This bill is author sponsored.

2) **Author's statement**: According to the author:

> In February of 2020, the State Auditor released a report that examined how well data collected from ALPRs is safeguarded. Although current law requires agencies to have a policy to protect data in ALPRs, Howle found that the four reviewed agencies either did not have a policy for ALPR usage, or the policy was deficient. None of the agencies had performed an audit on ALPR systems to detect any misuse. Agencies regularly share

ALPR data with other agencies, but none claimed to have first considered whether the receiving agency had a right and need for the data. Many of the agencies use cloud storage and believe that this storage is compliant with criminal justice information services (CJIS) policy. These agencies, however, could not demonstrate any vetting performed to confirm compliance with CJIS policy

3) **Automated license plate readers**: An ALPR system is one or more mobile or fixed cameras combined with computer algorithms that can read and convert images of automobile registration plates, and the characters they contain, into computer-readable data showing the license plate itself, as well as the time, date, and place of the picture. ALPR systems can also provide a “contextual” photo of the car itself, making information about car make and model, distinguishing features, state of registration, and individuals in the car available as well. ALPR systems operate by automatically scanning any license plate within range. Some ALPR systems can scan up to 2,000 license plates per minute. In the private sector, ALPR systems are used to monitor parking facilities and assist repossession companies in identifying vehicles. Some gated communities use ALPRs to monitor and regulate access.

   When used by law enforcement, each scanned license plate is checked against a variety of databases, such as the federal AMBER Alert for missing children, or the National Crime Information Center, which aggregates 21 different databases tracking categories such as stolen property, sex offenders, gang affiliates, and known violent persons. If one of the license plates photographed by the system gets a hit based on a match with one of the databases or some other “hot list,” the ALPR system can alert law enforcement in real time so they can take action.

   Prior to 2015, ALPR data was not considered personal information (PI). SB 34 (Hill, Ch. 532, Stats. 2015) created obligations for ALPR data for operators and end-users, and included ALPR data in the definition of PI for the purposes of California’s data breach notification law. That bill defined an ALPR “operator” to mean a person that operates an ALPR system, not including a transportation agency that employs electronic toll collection, as specified, and defined an ALPR “end-user” as a person that accesses or uses ALPR information, subject to certain exceptions.

4) **Law enforcement use of ALPR systems**: ALPR systems can be used to serve four specific public safety goals: (a) crime analysis; (b) alert law enforcement officials that a license plate number on a “hot list” is nearby; (c) monitor the movements of vehicles operated by individuals with travel restrictions; and (d) identify criminal conduct that was otherwise unnoticed. Hot lists, are generally databases of “vehicles of interest,” such as such as the plate numbers of stolen cars or cars suspected of being involved in crimes or gang activity. In some cases, especially in Texas, law enforcement will create a list of individuals with overdue court fees. That way, police receive real time updates when particular vehicles are spotted by an ALPR camera. Hot lists may be compiled by the local law enforcement agency using the ALPR system or by other state or federal government agencies.

   As recently reported by the Los Angeles Times, because law enforcement can buy data from private operators and databases, private surveillance databases of this data can be just as intrusive as government databases.

When someone drives down a street or parks a car at a curb, there is no expectation of privacy — the driver, the car and the license plate are in public view. Yet most people would recoil if the government announced a program to scan those license plate numbers into a database it could use to determine whose car was parked where and when. It's an obnoxiously intrusive idea that sneaks over the line between a free society and Big Brother dystopia. The notion that the government could trace people's travels whenever it wishes undercuts our fundamental belief that, barring probable cause to suspect involvement in a crime, we should be able to move about freely without being tracked.

But government agencies, from local police departments to Immigration and Customs Enforcement, are able to do just that. Some police agencies — including the Los Angeles Police Department and the Los Angeles County Sheriff's Department — maintain their own databases of scanned plates, which is problematic enough without proper policies and controls in place. Many share with other agencies in broad networks. Some agencies contract with private vendors that build massive databases by merging feeds from automatic license plate readers. So while police must obtain a warrant before placing a tracking device on someone's car, they do not need a judge's permission to contract with a database — or build their own — and, theoretically, track a person's movements over time by consulting records of where his or her car has been spotted.[1]

As described in this Committee's analysis of SB 34, these databases are also big business. One of the most well-known companies in this space, Livermore-based Vigilant Solutions, "has seen its appeal among law enforcement officers grow because it can offer police departments access to a trove of more than 2 billion scans, maintained by an affiliated company, Digital Recognition Network. That database is fed by cameras attached to vehicles driven by repossession agents roving the nation's roadways. The two companies have 160 employees. Vigilant reports having more than 3,500 law enforcement clients that either use the company's cameras or access its data. Digital Recognition Network has more than 250 customers. A Vigilant representative estimated that the entire industry brings in as much as $500 million a year."[2]

A 2011 transportation budget trailer bill restricted the use of ALPR technology by the CHP. Pursuant to AB 115 (Committee on Budget, Ch. 38, Stats. 2011), the CHP is only authorized to retain data captured by ALPR systems for 60 days, except where the data is being used for felony investigations or as evidence. The CHP is also prohibited from selling the data for any purpose or making the data available to an agency or person other than law enforcement agencies or officers. The data may only be used by law enforcement agencies for purposes of locating vehicles or persons reasonably suspected of being involved in the commission of a public offense. The CHP is required to monitor the internal use of ALPR data to prevent unauthorized use, and to regularly report to the Legislature on its ALPR practices and uses.

5) **Auditor's report calls for more oversight with regard to law enforcement use of ALPR**: In response to the growing concerns with ALPR systems, the Joint Legislative Audit

[1] Times Editorial Board, *Private surveillance databases are just as intrusive as government ones,* L.A. Times (Feb. 3, 2018.

[2] Faturechi, *Use of license plate photo databases is raising privacy concerns*, LA Times, (May 16, 2014).

Committee tasked the California State Auditor with conducting an audit of law enforcement agencies' use of ALPR systems and data.[3]

The report focused on four law enforcement agencies that have ALPR systems in place. The report 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." In addition, the audit found that three of the four agencies failed to establish ALPR policies that included all of the elements required by SB 34. All three failed to detail who had access to the systems and how they will monitor the use of the ALPR systems to ensure compliance with privacy laws. Other elements missing were related to restrictions on the sale of the data and the process for data destruction. The fourth entity, the Los Angeles Police Department, did not even have an ALPR policy.

The Auditor's report calls into question how these systems are being run, how the data is being protected, and what is being done with the data. The report reveals that agencies commingled standard ALPR data with criminal justice information and other sensitive PI about individuals, heightening the need for stronger security measures and more circumscribed access and use policies.

The Auditor additionally had difficulty determining whether the agencies made informed decisions about sharing the ALPR data at all because of deficient record keeping. Two of the agencies reviewed approved sharing ALPR data with hundreds of entities and one shared ALPR data with over a thousand. The sharing occurred with most of the other 49 states and included public and private entities.

For the most part, agencies relied on Vigilant Solutions software and protocols rather than establishing their own protocols and safety measures. The report indicates that for the agencies partnering with Vigilant, it was not clear who owns the data stored in the Vigilant cloud. In addition, serious security concerns were identified with the agencies using Vigilant, including the lack of contractual guarantees that the data will be stored in the United States or that adequate safeguards will be implemented.

Because of the many issues identified by the Auditor related to law enforcement's deficient ALPR policies, the report recommended that the Legislature direct the DOJ to develop a policy template that local law enforcement agencies can use as a model for their ALPR policies. This bill would now codify that recommendation.

This recommendation would also be codified by SB 210 (Wiener), which is co-sponsored by the Electronic Frontier Foundation and the Media Alliance and supported by a number of privacy and consumer advocacy organizations. Staff notes that SB 210 includes a number of provisions in addition to the recommendation that the DOJ develop a model ALPR policy, such as requiring ALPR operators and end-users to conduct annual audits to review ALPR searches, and requiring operators or end-users that are public agencies to destroy all ALPR

[3] *Automated License Plate Readers, To Better Protect Individuals' Privacy, Law Enforcement Must Increase Its Safeguards for the Data It Collects* (February 2020) California State Auditor, https://www.auditor.ca.gov/pdfs/reports/2019-118.pdf [as of Mar. 4, 2021].

data that does not match information on a hot list within 24 hours. To the extent that there is overlap between this bill and SB 210, the authors should work collaboratively as the bills move through the legislative process to ensure that the DOJ is ultimately not subject to duplicative requirements.

6) **Related legislation**: SB 210 (Wiener) *See* Comment 5.

7) **Prior legislation**: SB 1143 (Wiener, 2020) was substantially similar to SB 210. It was held in the Senate Transportation Committee.

   AB 1782 (Chau, 2019) would have required those operating ALPR systems and those accessing or using ALPR data to have policies that include procedures to ensure nonanonymized ALPR information is timely destroyed, except as specified, and that all ALPR information that is shared is anonymized. The bill was subsequently gutted and amended to address a different topic. It died in the Senate Appropriations Committee.

   SB 34 (Hill, Ch. 532, Stats. 2015) *See* Comment 3.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file

Opposition

None on file

Analysis Prepared by: Nichole Rocha / P. & C.P. / (916) 319-2200