Date of Hearing: April 23, 2019

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 1782 (Chau) – As Amended April 10, 2019

SUBJECT: Automated license plate recognition information: privacy policy

SUMMARY: This bill would require automated license plate recognition (ALPR) end-users to amend their privacy policies to require the destruction of ALPR information after 60 days, and to prohibit the sharing of non-anonymized ALPR information, as specified. Specifically, **this bill would**:

1) Require an end-user that holds ALPR information to amend its usage and privacy policy to include a procedure to ensure the destruction of all non-anonymized ALPR information no more than 60 days from the date of collection.

2) Require an end-user that holds ALPR information to amend its usage and privacy policy to include a procedure to ensure that all ALPR information shared with an agency, organization, or individual outside of the entity that generated that information is sufficiently anonymized to protect the privacy of the license plate holder.

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) Authorizes the California Highway Patrol (CHP) to retain license plate data captured by an ALPR reader for not more than 60 days, unless the data is being used as evidence or for felony investigations, including but not limited to, auto theft, homicides, kidnapping, burglaries, elder and juvenile abductions, Amber Alert, and Blue Alerts. (Veh. Code Sec. 2413(b).)

3) Prohibits CHP from selling ALPR data or sharing it with anyone other than a law enforcement agency or law enforcement officer. Specifies that a law enforcement agency may only use ALPR data for purposes of locating vehicles or persons reasonably suspected of being involved in the commission of a public offense. Requires CHP to monitor internal use of ALPR data to prevent unauthorized use. (Veh. Code Sec. 2413(c).)

4) Requires an "ALPR operator," as defined, 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. (Civ. Code Sec. 1798.90.51.)

5) Requires an ALPR end-user, as defined, 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. To further this end, the ALPR end-user must implement a prescribed usage and privacy policy that specifies, among other things, how long the ALPR end-user may retain the information and how the information is used. (Civ. Code Sec. 1798.90.53.)

6) Requires, pursuant to the Data Breach Protection Law, a public agency, or a person or business conducting business in California, that owns or licenses computerized data that includes personal information to disclose a breach of the security of the system or data 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. (Civ. Code Secs. 1798.29 and 1798.82.)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Purpose of the bill**: This bill seeks to protect individuals' privacy by prohibiting ALPR end-users from sharing non-anonymized ALPR data, and by requiring the destruction of that data within 60 days of its collection, subject to certain exceptions. This is an author-sponsored bill.

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

> Current law requires that [ALPR] end-users provide usage and privacy policies for the security of any data that is collected (both in terms of the storage and access), destroy any non-investigative data, and make their policies easily accessible to the public. However, current law is vague and does not provide the public with the accountability of knowing their information is safe. […]
>
> AB 1782 would require that all non-anonymized ALPR data be destroyed after 60 days, and […] would further require that ALPR data be anonymized if it is shared with an outside entity, other than the entity that generated the data.

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. This bill now seeks to prohibit end-users from sharing ALPR data unless it is anonymized, and would require end-users to delete any ALPR data within 60 days from the date of collection.

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

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

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.

By requiring ALPR data to be deleted after 60 days from collection, this bill seeks to apply the same standard employed by the CHP to public and private entities alike. The California State Sheriffs Association argues in opposition that this bill impedes any benefit of sharing ALPR data by requiring shared data to by anonymized, and by requiring its deletion.

> Law enforcement agencies across the state and nation have used ALPR data to solve crimes and apprehend criminal suspects. While some cases are solved quickly using this technology, it can also be exceptionally helpful in solving crimes that have occurred deeper in the past. To set an arbitrary data destruction timeline such as 60 days in statute will hinder the use of a valuable law enforcement tool. Additionally, by effectively stopping the use of ALPR data sharing among law enforcement agencies and other collectors of the data, AB 1782 hampers a major virtue of the technology inasmuch as it provides information regarding the whereabouts of objects that are transient by nature. For these reasons, we must respectfully oppose AB 1782.

Given that the government requires all car, truck, and motorcycle drivers to display license plates in public view, it is especially important that privacy be taken into account when considering the regulation of this type of data. It is particularly disturbing that ALPR systems track and record the movements of millions of ordinary people, even though the overwhelming majority are not connected to a crime. That being said, ALPR data can be incredibly useful to law enforcement. The following amendment would remove agencies from the prohibition on sharing non-anonymized ALPR data, but would not remove the 60-day destruction policy for ALPR data. This both more accurately mirrors the restrictions currently imposed on the CHP, but also arguably strikes the right balance between protecting individuals' privacy, and allowing law enforcement to use new technologies that can increase public safety.

> Author's amendment:
>
> On page 4, line 15, strike "agency"

5) **Anonymization of ALPR data**: In 2017, the American Civil Liberties Union (ACLU) and Electronic Frontier Foundation filed a case against the Los Angeles Police Department and

the Los Angeles Sheriff's Department, seeking to compel the departments to disclose all ALPR data collected during a one-week period pursuant to a California Public Records Act (CPRA) request. Petitioners sought disclosure of this ALPR data "so that the legal and policy implications of the government's use of ALPRs to collect vast amounts of information on almost exclusively law-abiding [citizens of Los Angeles] may be fully and fairly debated." Recognizing that the CPRA should be interpreted in light of modern technological realities, the court found that law enforcement may not withhold this data under the investigatory exemption in the CPRA, because the "scans are not conducted as part of a targeted inquiry into any particular crime or crimes." (*ACLU Foundation of Southern California v. County of Los Angeles* (2017) 221 Cal.Rptr.3d 832; hereinafter *ACLU v. Los Angeles County*.)

When considering the trial court's analysis of the "catch all" provision of the CPRA (Gov. Code Sec. 6255(a)), which permits an agency to withhold a public record if the agency demonstrates that on the facts of the particular case the public interest served by *not* disclosing the record clearly outweigh the interest served by disclosure of the record, the trial court held that raw ALPR data could be withheld because the balance of interests (at least in part, because of the privacy implications) weighed clearly against disclosure of raw ALPR data. The trial court reached the same conclusion for anonymized data. Finding that the trial court erred in in reaching this last conclusion, the Supreme Court remanded the case to the trial court to re-consider the question of whether anonymized data may be withheld despite a CPRA request, under that law's catch all provision. (*ACLU v. Los Angeles County* at 441.)

In the past, this Committee has raised concerns about bills that interfere with pending litigation, as any such interference could prevent a court from deciding an action based upon the laws in place at the time the cause of action accrued or create a situation where the legislative branch is used to circumvent the discretion and independence of the judicial branch. While *ACLU v. Los Angeles County* was remanded so the court may re-consider whether anonymized ALPR data may be withheld from disclosure in response to a CPRA request, requiring anonymization of ALPR data before it may be shared by an end-user does not interfere with that case. In other words, this bill does not interfere with pending litigation because it does not amend the CPRA to settle that question before the court in the ACLU case. Moreover, the court has already determined that raw ALPR data cannot be disclosed pursuant to a CPRA request. The court is now tasked with determining whether anonymized data will receive the same treatment under the CPRA. This bill would not prohibit a law enforcement agency from possessing anonymized data or disclosing it pursuant to a CPRA request if the court decides such information is disclose-able.

That being said, there are legitimate concerns related to whether ALPR data can be sufficiently anonymized to protect individuals' privacy. Because license plate numbers can be associated with the owner of a car, it appears that the only way to truly anonymize ALPR data is to scramble (or redact) the license plate numbers. Given the other information collected by ALPR systems, such as time, date, and location, even anonymized ALPR data may be "re-identifiable" when combined with other information. By requiring all end-users (and operators, as discussed more in Comment 6, below) to delete ALPR data within 60 days from the time of collection, this bill would arguably limit the information that people can use to re-identify ALPR data as well.

6) **Bill imposes obligations on end-users but not operators**: As noted in Comment 3, above, existing law defines 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 defines an ALPR "end-user" as a person that accesses or uses ALPR information, subject to certain exceptions.

The L.A. Times recently reported that ALPR data is being used by Immigration and Customs Enforcement (ICE) to track undocumented immigrants. At the center of the controversy is a company, Vigilant Solutions, who has long been scrutinized for the volume of ALPR data it amasses and sells.

> Civil rights groups in California want police and sheriff's departments to stop sending license plate scanner information to a national private database, saying new public documents show federal immigration agents are using the system in breach of sanctuary state and city laws.
>
> The American Civil Liberties Union of Northern California, which obtained the documents as part of an open records lawsuit against U.S. Immigration and Customs Enforcement, is calling on lawmakers to request a statewide audit to review the data-sharing practices.
>
> The collection of more than 1,000 pages of contracts, emails, manuals and other materials shows some California law enforcement departments have granted ICE unfettered access to the personal data of drivers and that federal officials are using it to track and locate immigrants in the country illegally who might not have criminal records and could be protected under the state's sanctuary and privacy policies. […]
>
> The documents obtained by the ACLU provide the deepest look yet into the database run by Vigilant Solutions, one of the largest suppliers of data analysis software and equipment for police and sheriff's departments across the country. They show more than 9,000 ICE agents nationwide have access to the Vigilant system through a $6.1-million contract with Thomson Reuters Special Services that was signed in December 2017 and runs through September 2020. (Ulloa, *ICE is tracking immigrants with the help of California sanctuary cities, court records show*, L.A. Times (Mar. 13, 2019).)

Another L.A. Times article describes the problems that Vigilant and similar companies create, even outside of the immigration context:

> We have been concerned about the broad spread of license-plate scanners in recent years primarily because of the potential for ubiquitous monitoring. Clearly, a database that allows police to, in essence, go back in time and see what cars might have been parked outside a store as it was being robbed could be a useful investigative tool. But at what cost?
>
> Under this privatized system, government officials can enter a license plate and receive an alert as soon as it turns up on any of the nationwide army of scanners — in police cars, on utility poles, in cars driven by private citizens working with the vendors — that feed these databases. Because the data is not purged after a short amount of time, it also means police can plug in a license plate and find out where a car had traveled on any specific day going back years. Such an arrangement might pass constitutional muster, but it certainly violates our right and expectation to not have our daily activities collected and saved for retrieval by government agents.

> The top company selling such data, Vigilant Solutions — which claims more than 5 billion archived detections and another 150 million added monthly — is under no obligation to purge license-plate captures after a reasonable period of time. And there are no legal restrictions on to whom it may sell access. Such companies tend to cater to government agencies, insurance companies, collections agencies and other businesses with an interest in figuring out where a specific car has been. But they could easily decide to fully democratize access by selling the service to individuals. Imagine the repercussions if someone could create an account, pay a fee, enter a license plate number and establish an alert for every time and place the vehicle pops up on a scanner. It's a stalker's delight. (Times Editorial Board, *Private surveillance databases are just as intrusive as government ones*, L.A. Times (Feb. 3, 2018).)

To that end, this bill would require end-users to delete ALPR data within 60 days after it has been collected. Arguably, the author intends to limit the amount of ALPR data companies like Vigilant Solutions can collect and sell, but, according to Vigilant's website, it merely *stores* information from operators on the cloud. Further complicating this issue, not all ALPR "operators" are private entities like Vigilant. For example, the Santa Clara District Attorney's Office, which describes itself as an "end-user" and states that it accesses ALPR information "from systems controlled by private and outside law enforcement ALPR operator agencies." Thus, it appears that law enforcement agencies could be either ALPR "operators" or ALPR "end users," or both. Consider also, for example, the Northern California Regional Intelligence Center (NCRIC). NCRIC refers to itself as a "multi-jurisdiction public safety program" that assists local, state, federal, and tribal public safety agencies with analysis, and its board members appear to be members of local law enforcement. Since NCRIC operates cameras and gathers information, it would be an "operator." However, to the extent that members share this data among themselves for law enforcement purposes, it could also be an "end-user."

The following amendment would apply the anonymization and deletion requirements of the bill to "operators" as well as end-users, thereby better effecting the author's intent to limit the ALPR data that can be amassed and shared by private and public entities alike. The amendment would also reflect the prior amendment that the author accepted in Comment 4, above, ensuring that law enforcement may receive non-anonymized ALPR data.

> Author's amendment:
>
> Civ. Code Sec. 1798.90.51 is amended to read, in relevant part: (b)(2)(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.~~ *A procedure to ensure the destruction of all nonanonymized ALPR information no more than 60 days from the date of collection, except as authorized pursuant to Section 2413 of the Vehicle Code.*
>
> *(H) A procedure to ensure that all ALPR information that is shared with an organization, or individual outside of the entity that generated that information is sufficiently anonymized to protect the privacy of the license plate holder.*

7) **Prior legislation**: SB 35 (Hill, Ch. 532, Stats. 2015) *See* Comment 3.

   SB 893 (Hill, 2014) would have placed restrictions on the use of ALPR technology by both public-sector and private-sector users, in a manner similar to this bill. SB 893 failed passage on the Senate Floor.

   SB 1330 (Simitian, 2011) would have placed restrictions on the use of license plate recognition LPR technology by private entities, including restrictions on the retention, use, and sale of such data. SB 1330 failed passage on the Senate Floor.

   AB 115 (Committee on Budget, Ch. 38, Stats. 2011) allows the CHP to retain data captured by ALPR systems for no more than 60 days, and also prohibits the CHP from selling ALPR data or making it available to anyone other than law enforcement agencies.

   SB 854 (Committee on Budget and Fiscal Review, 2010) would have authorized the CHP to retain ALPR data for not more than 72 hours unless the data is being used as evidence or for a legitimate law enforcement purpose, and also would have prohibited CHP from selling ALPR data or making the data available to an agency that is not a law enforcement agency or an individual that is not a law enforcement officer. SB 854 failed passage on the Senate Floor.

   AB 1614 (Committee on Budget and Fiscal Review, 2010) would have authorized the CHP to retain ALPR data for not more than 72 hours unless the data is being used as evidence or for a legitimate law enforcement purpose, and also would have prohibited CHP from selling ALPR data or making the data available to an agency that is not a law enforcement agency or an individual that is not a law enforcement officer. AB 1614 failed passage on the Senate Floor.

8) **Double-referral**: This bill was double-referred to the Assembly Judiciary Committee where it was heard on April 9, 2019, and passed out on a 9 – 1 vote.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file

Opposition

California State Sheriffs Association

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