SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2023-2024 Regular Session

AB 3138 (Wilson)
Version: June 18, 2024
Hearing Date: July 2, 2024
Fiscal: Yes
Urgency: No
CK

SUBJECT

Vehicle identification and registration: license plates

DIGEST

This bill authorizes alternative, digital license plates to include vehicle location technology.

EXECUTIVE SUMMARY

SB 806 (Hueso, Ch. 569, Stats. 2013) provided the DMV authorization to establish a pilot program to evaluate the use of alternatives to the stickers, tabs, license plates, and registration cards that were already authorized by the Vehicle Code, subject to specified requirements. Any pilot program so established was to be completed by January 1, 2017 with required reporting due July 1, 2018. Those dates were pushed back by a series of bills over the years due to low participation by users and the companies making the products. Three companies participated in the pilot: one for a digital plate, one for a vinyl frontal plate, and one for a digital registration card. AB 984 (Wilson, Ch. 746, Stats. 2022) established a permanent program as of January 1, 2023, for the adoption of alternative devices, including digital license plates and registration cards.

One major concern with AB 984 was its authorization of vehicle location technology being used in the digital plates and the serious privacy and safety concerns attendant with that. Ultimately, a compromise was reached that such technology could only be used in certain fleet or commercial vehicles with protections against employers monitoring employees, but otherwise such technology was barred in other plates.

This bill now explicitly authorizes vehicle location technology to be placed in these plates. Most of these plates are provided by one company in California, Reviver, which recently had a major security vulnerability exposed. No timely support was received by the Committee. The bill is opposed by a coalition of privacy, consumer, and domestic violence prevention groups, including the California Partnership to End Domestic

Violence, that raise privacy, security, and equitability concerns with the bill. The bill passed out of the Senate Transportation Committee on a 14 to 0 vote.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Authorizes the DMV to issue one or more stickers, tabs, or other suitable devices in lieu of the license plates provided for under the Vehicle Code. Except when the physical differences between the stickers, tabs, or devices and license plates by their nature render the provisions of the Vehicle Code inapplicable, all provisions relating to license plates may apply to stickers, tabs, or devices. (Veh. Code § 4853(a).)

2) Requires the DMV to establish a program authorizing an entity to issue devices as alternatives to the conventional license plates, stickers, tabs, and registration cards authorized by the Vehicle Code, subject to all of the following requirements:
    a) The alternative device is subject to the approval of the DMV and CHP and may be used in lieu of a device issued by the DMV.
    b) Except as specifically authorized, an alternate device shall not include vehicle location technology. The DMV is required, by no later than January 1, 2024, to recall any devices with vehicle location technology that have been issued, to vehicles other than those below.
    c) Notwithstanding the above, vehicle location technology may be offered for vehicles registered as fleet vehicles, commercial vehicles, and those operating under an occupational license if capable of being disabled by the user. (Veh. Code § 4854(a).)

3) Requires any device with vehicle location technology to display a visual indication that it is in active use. (Veh. Code § 4854(a).)

4) Requires any data exchanged between the DMV and the device, or the provider of the device, to be limited to that data necessary to display evidence of registration compliance, including the payment of registration fees, plate configurations, and the information or images displayed on the alternative product. (Veh. Code § 4854(a).)

5) Prohibits the DMV from receiving or retaining directly from an alternative device authorized hereby or the provider of the alternative device any electronic information regarding the movement, location, or use of a vehicle or person with an alternative device. (Veh. Code § 4854(a).)

6) Provides that use of the alternative device must be optional, and users shall affirmatively opt in to using the alternative device instead of a conventional license plate, sticker, tab, or registration card. (Veh. Code § 4854(a).)

7) Requires the DMV to adopt regulations to carry out this program. (Veh. Code § 4854(b).)

8) Permits the DMV to authorize approved environmental or specialized license plates to be displayed on an alternative device. (Veh. Code § 4854(b)(8).)

9) Establishes the California Consumer Privacy Act of 2018 (CCPA), which grants consumers certain rights with regard to their personal information, including enhanced notice, access, and disclosure; the right to deletion; the right to restrict the sale of information; and protection from discrimination for exercising these rights. It places attendant obligations on businesses to respect those rights. (Civ. Code § 1798.100 et seq.)

This bill:

1) Removes the prohibition on equipping these digital plates with vehicle location technology and authorizes such technology in these plates that complies with the requirements of the bill and has all of the following features:
    a) The technology is capable of being permanently disabled by means of a nonreversible method that ceases all vehicle location functionality and tracking information capabilities.
    b) The technology is capable of being manually disabled and enabled by a driver of the vehicle while that driver is inside the vehicle.
    c) The method of manually disabling and enabling the vehicle location technology shall be prominently located and easy to disable, without requiring access to a remote, online application and shall not require a password or log-in information.
    d) Once the vehicle location technology is manually disabled from inside the car, the only method of reenabling the technology shall be manually from inside the car. The registered owner of the license plate, the manufacturer, the Department of Motor Vehicles, or any other entity shall not have the capability of reenabling the vehicle location technology through remote means.

2) Permits the DMV to authorize an alternative plate to replicate a specialized license plate or a license plate requiring an occupational license.

3) Requires the DMV, by December 31, 2025, to report to the Legislature on the state's authority to regulate the content and messaging on traditional and digital license plates. The report shall consider the state's authority under both state and

federal law, including the Communications Decency Act of 1996 (47 U.S.C. Sec. 230). The report shall include an analysis regarding the seven identifying characters and any additional messaging or signage that may be authorized. This report may include recommendations on relevant state policy regarding authorization of messaging on digital license plates, including any restrictions or constraints.

COMMENTS

1. Authorization of digital license plates

As indicated, the DMV was authorized and did establish a pilot program to evaluate alternative devices. In conjunction with CHP, the DMV tested three products, an electronic registration card, a license plate wrap, and a digital license plate. Participation in the pilot for the first two devices only grew to approximately 100 and 300 vehicles, respectively, from the start of the program to the cutoff for the DMV's required report. The digital license plate pilot started with five vehicles and only reached 85 by 2017. However, over the following two years the pilot expanded to 1,500 vehicles.

AB 984 provided authority for the permanent establishment of such alternative device programs. It laid out a series of requirements that the program will need to comply with. The alternative license plates must also abide by all provisions of the Vehicle Code relating to license plates, except where physical differences render them inapplicable. The digital registration cards must also comply with the laws currently applying to registration cards. The law applies various visibility and legibility requirements on the devices intended to serve in lieu of license plates. Where there is an identified need, the DMV is authorized to establish additional requirements and regulations to implement the program.

2. Authorizing vehicle location technology despite the risks

Relevant here, the law currently prohibits these alternative, digital license plates from including vehicle location technology except in limited circumstances for fleet vehicles and other commercial vehicles. This language was added to AB 984 after a large coalition of privacy, consumer, and domestic violence prevention organizations came out in strong opposition to the language in the bill that allowed for this technology. The coalition highlighted that it puts certain vulnerable groups at serious risk, including domestic violence survivors, LGBTQ teens, those seeking reproductive care, and undocumented Californians.

These concerns were well-founded as more reports have found that vehicle location technology has serious privacy and security issues that can lead to constant surveillance

and victimizes individuals through their vehicles. This troubling trend was also reported on by the New York Times:

> A car, to its driver, can feel like a sanctuary. A place to sing favorite songs off key, to cry, to vent or to drive somewhere no one knows you're going. But in truth, there are few places in our lives less private.
>
> Modern cars have been called "smartphones with wheels" because they are internet-connected and have myriad methods of data collection, from cameras and seat weight sensors to records of how hard you brake and corner. Most drivers don't realize how much information their cars are collecting and who has access to it, said Jen Caltrider, a privacy researcher at Mozilla who reviewed the privacy policies of more than 25 car brands and found surprising disclosures, such as Nissan saying it might collect information about "sexual activity."[1]

One horrifying example involved a woman tracked through her Tesla by her abusive husband who placed a baseball bat in her backseat.[2] This is a growing problem:

> Cases of technology-enabled stalking involving cars are emerging as automakers add ever-more-sophisticated features, such as location tracking and remote control of functions such as locking doors or honking the horn, according to interviews with divorce lawyers, private investigators and anti-domestic-violence advocates. Such abusive behavior using other devices, such as phone spyware or tracking devices, has long been a concern, prompting technology companies including Google and Apple to design safeguards into their products.[3]

In fact, a number of bills have sought to place guardrails on the remote vehicle technology used in vehicles to protect against these serious concerns, including SB 1000 (Ashby, 2024), SB 1394 (Min, 2024), and AB 3139 (Weber, 2024).

Ultimately, a compromise was reached on AB 984 in 2022 limiting the use of such technology only to plates for specified commercial vehicles. The coalition went neutral and wrote commending the author for ensuring "that these license plates cannot be used to track domestic violence survivors, LGBTQ teens, people coming to California for healthcare banned in their state, and others."

---

[1] Kashmir Hill, *Your Car Is Tracking You. Abusive Partners May Be, Too.* (December 31, 2023) The New York Times, https://www.nytimes.com/2023/12/31/technology/car-trackers-gps-abuse.html. All internet citations are current as of June 25, 2024.
[2] Kristina Cooke & Dan Levine, *An abused wife took on Tesla over tracking tech. She lost.* (December 19, 2023) Reuters, https://www.reuters.com/technology/an-abused-wife-took-tesla-over-tracking-tech-she-lost-2023-12-19/.
[3] *Ibid.*

Now, less than two years later, this bill, championed by the maker of these plates, Reviver, again authorizes the use of vehicle location technology.

According to the author: "AB 3138 will provide consumers with the choice of opting into GPS enabled alternative registration devices, or digital plates while providing levels of privacy protections above and beyond those that exist in current law for comparable GPS enabled products, including cars themselves."

A coalition in opposition, including the California Partnership to End Domestic Violence, the Consumer Federation of America, and the Electronic Frontier Foundation, expresses their grave concerns with the bill:

> Including GPS tracking capability into digital license plates threatens to hurt people in vulnerable positions. For example, A.B. 3138 would jeopardize the safety of those traveling to California from a state that criminalizes abortions. People may not be aware that a rideshare vehicle is recording their drive to a Planned Parenthood clinic, or be unable to convince a driver to disable tracking that could generate data that can be used as evidence against them in a state where abortion is criminalized. Similarly, Immigrations and Customs Enforcement (ICE) could use the GPS surveillance technology to track and locate immigrants, as it has done with other location tracking devices. Unsupportive parents of queer youth could use GPS-loaded plates to monitor whether teens are going to local LGBTQI Centers or events—or use the threat of pervasive tracking as a way to keep young people from seeking support in the first place. Finally, there are serious implications in domestic violence situations, where GPS tracking is already being abused. For example, two Kansas City families are jointly suing the company Spytec GPS after its technology was used in a double-murder suicide, in which a man used GPS trackers to find and kill his ex-girlfriend, her current boyfriend, and then himself. The families say the lawsuit is, in part, to raise awareness about the danger of making this technology and location information more easily available.
>
> Additionally, these plates raise software security concerns. While any qualified company can apply to provide these plates, currently the only vendor in California is Reviver. Shortly after A.B. 984 became law, researchers uncovered that Reviver had an alarming security vulnerability in its systems that made it possible for infiltrators to track vehicles by GPS in real time and even change what the plates displayed. The company's goal is to modernize personalization and safety with digital license plate technology for passenger vehicles. Yet it has failed once to competently secure the location data collected by its products. How can we trust this company to completely protect the sensitive location information for

> people seeking abortions, LGBTQI teens, immigrants, and survivors of domestic violence today?

As mentioned by opposition, the company behind nearly all of these plates in California and the champion of this bill, Reviver, was recently subject to a massive security compromise:

> California is the latest adopter of the technology, following Arizona, Michigan, and Texas in launching its own digital license plate program in October 2022. But residents should think twice before opting into the new technology.
>
> That's because a team of web security researchers led by Sam Curry found weaknesses in the software built into the Reviver-supplied California license plates, the company leading the push for digital plates. Thanks to the SIM card found in the plates, these web security experts were able to easily hack into the administrative back end of Reviver.
>
> The team explained their hacking process in a thoroughly technical blog post and, while the developer jargon doesn't mean much to the average car owner, **it's clear just how vulnerable these digital plates are**.
>
> Once the team established full administrative access, they could see the details of every user's account, including vehicle type and physical address. Every vehicle with a Reviver plate could also be tracked by GPS in real-time, and the hackers could change or add any slogan to the plate. Additionally, the security function of the plates that label the car as stolen could be abused, allowing hackers to mislabel the vehicle as stolen at a moment's notice.
>
> Fleet management functions were also easy targets, with the hackers able to locate and manage all vehicles across a number of companies' fleets. This could become problematic for vehicles bearing dealer tags, as the hackers could easily wipe those identifications away. One of the most glaring issues found in the investigation was that consumer and commercial tags could be simply deleted by bad actors.[4]

Despite the provisions outlining certain disabling mechanisms in connection with these plates, the Committee may wish to consider whether more research should be done into whether these plates are safe and whether authorization for a company to embed more

---

[4] Emmet White, *Hackers Gained Access To California's Digital License Plates* (January 11, 2023) Autoweek, https://www.autoweek.com/news/technology/a42444153/california-digital-license-plates-hacked/. Emphasis added.

intrusive technology is appropriate given the recent, widespread security compromise at that very company in connection with this product.

Oakland Privacy writes in opposition:

> To add a massive collection of highly sensitive geolocation data - by a company that has already experienced a severe breach of security - as an official act of the state – is ill-advised and Irresponsible. Regardless of whether the vendor solemnly assures us that it will never happen again, just as they solemnly advised us it could never happen before it did.
>
> California has to be able to assure people that the products they are referred to from the Department of Motor Vehicles are safe and secure and that is simply impossible to say after the 2023 hacking. This should not be a "buyer-beware" situation. There is absolutely no convincing reason to make the situation degrees more dangerous for Californians by including the collection of "highly sensitive personal information", as defined under California law.
>
> Drivers have made clear for some time that they resent the collection of excess information from their car technology, and their inability to control where that information ends up. Just last week, General Motors announced they would stop sending driver data to the data broker Lexis Nexis after the NY Times revealed the practice. People don't like it and they won't like it the next time Reviver has a security problem and a river of Californian's geo-location data ends up for sale to the highest bidder.

SUPPORT

None received

OPPOSITION

Anti Police-Terror Project
California Partnership to End Domestic Violence
Consumer Federation of America
Electronic Frontier Foundation
Oakland Privacy
Privacy Rights Clearinghouse
Secure Justice

RELATED LEGISLATION

Pending Legislation:

SB 1000 (Ashby, 2024) *See* Comment 2.

SB 1394 (Min, 2024) *See* Comment 2.

AB 3139 (Weber, 2024) *See* Comment 2.

Prior Legislation:

SB 806 (Hueso, Ch. 569, Stats. 2013) *See* Executive Summary.

AB 984 (Wilson, Ch. 746, Stats. 2022) *See* Executive Summary and Comment 2.

PRIOR VOTES:

Assembly Floor (Ayes 65, Noes 0)
Assembly Appropriations Committee (Ayes 13, Noes 2)
Assembly Privacy and Consumer Protection Committee (Ayes 11, Noes 0)
Assembly Transportation Committee (Ayes 11, Noes 0)
****