

Date of Hearing: April 30, 2024

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION

Rebecca Bauer-Kahan, Chair

AB 2741 (Haney) – As Amended April 24, 2024

AS PROPOSED TO BE AMENDED

SUBJECT: Rental car companies: electronic surveillance technology

SYNOPSIS

California prohibits rental car companies from using, accessing, or obtaining any information relating to a customer's use of the rental vehicle that was obtained using electronic surveillance technology, except in a few narrowly defined situations including when the customer fails to return the vehicle within three days of the contracted return date. This bill seeks to shorten the time period that a rental car company must wait before accessing surveillance technology in vehicles that have not been returned by the end of the contract period from three days to one day.

The bill currently in print goes beyond allowing rental car companies to activate surveillance technology faster to locate rental cars when they are not returned on time: it would also allow rental car companies to freely use surveillance technology to collect information on their customers for any purpose, so long as the company included a notice in the rental agreement. Because this is not the author's intent and it would undermine longstanding privacy protections, the author has agreed to remove this provision.

This bill is supported by the American Car Rental Association and the California Travel Association. Oakland Privacy is opposed to the provisions that the proposed amendments would remove.

SUMMARY: Decreases the time that a rental company must wait after the contracted or extended return date before activating electronic surveillance technology to 24 hours, and would remove the 24-hour notice requirement prior to activating the electronic surveillance technology. Specifically, **this bill:**

- 1) Authorizes rental car companies to enable electronic surveillance technology if a rental car has not been returned more than 24 hours after the contracted return date or following the end of a contract extension.
- 2) Eliminates the requirement that renters acknowledge that they understand that the technology may be activated if they fail to return the vehicle and the requirement that the information be provided orally to the renter at the time the lease agreement is executed.
- 3) Requires that the information related to surveillance technology be provided to the renter in the rental or lease agreement.
- 4) Presumes that a renter has no liability for any loss due to theft if an authorized driver has possession of the ignition key furnished by the rental company.

EXISTING LAW:

- 1) Provides that, among other rights, all people have an inalienable right to pursue and obtain privacy. (Cal. Const., art.1, § 1.)
- 2) Governs the obligations arising from rental passenger vehicle transactions. (Civ. Code § 1939.01 et seq.)
- 3) Prohibits a rental car company from using, accessing, or obtaining any information relating to the renter's use of the rental vehicle that was obtained using electronic surveillance technology, except in limited circumstances. (Civ. Code § 1939.23(a).)
- 4) Provides that rental car companies are permitted to use electronic surveillance technology in response to a specific request from law enforcement pursuant to a subpoena or search warrant or for the purpose of locating a stolen, abandoned, or missing rental vehicle after one of the following:
 - a) The renter or law enforcement has informed the rental car company that the vehicle is missing or has been stolen or abandoned.
 - b) The rental vehicle has not been returned following 72 hours after the contracted return date or one week after the end of an extension of that return date.
 - c) The rental car company discovers that the vehicle has been stolen or abandoned and, if stolen, reports the vehicle stolen to law enforcement by filing a stolen vehicle report, unless law enforcement has already informed the rental company that the vehicle is missing or has been stolen or abandoned.
 - d) The rental vehicle is the subject of an AMBER Alert issued pursuant to Section 8594 of the Government Code. If the rental company uses the equipment in connection with this provision relating to an AMBER Alert, the rental company shall notify law enforcement that one of the rental company's vehicles is the subject of an AMBER Alert upon becoming aware of the situation, unless law enforcement has already informed the rental company that the vehicle was the subject of an AMBER Alert. (Civ. Code § 1939.23(a).)
- 5) Requires a rental car company to maintain a record of information relevant to the activation of electronic surveillance technology, including information regarding communications with the renter and law enforcement. Existing law specifies that this information shall include the return date, the date and time the electronic surveillance technology was activated, and, if relevant, a record of written or other communication with the renter, including communications regarding extensions of the rental, police reports, or other written communication with law enforcement officials. (Civ. Code § 1939.23(a)(1)(B).)
- 6) Permits a rental company to equip its rental vehicles with certain electronic surveillance technology, but prohibits the rental company from using, accessing, or obtaining any information relating to the renter's use of the rental vehicle that was obtained using the electronic surveillance technology, except:
 - e) To discover or repair a defect in global positioning systems (GPS)-based technology that provides navigation assistance to the occupants of the rental vehicle.
 - f) To allow for the remote locking or unlocking of a vehicle at the request of the renter.

- g) To provide roadside assistance, such as towing, flat tire, or fuel services at the request of the renter.
 - h) For the sole purpose of determining the date and time the vehicle departs from or is returned to the rental company, and the total mileage driven and the vehicle fuel level of the returned vehicle. (Civ. Code § 1939.23(b)-(c).)
- 7) Prohibits a rental car company from using electronic surveillance technology to track a renter in order to impose fines or surcharges relating to the renter's use of the rental vehicle. (Civ. Code § 1939.23(d).)

FISCAL EFFECT: As currently in print, this bill is keyed non-fiscal.

COMMENTS:

1) **Purpose of this bill.** California prohibits rental car companies from using, accessing, or obtaining any information relating to a customer's use of the rental vehicle that was obtained using electronic surveillance technology, except in a few narrowly defined situations including when the customer fails to return the vehicle within three days of the contracted return date. This bill seeks to shorten the time period that a rental car company must wait before accessing surveillance technology in vehicles that have not been returned by the end of the contract period from three days to one day.

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

Car theft in the State of California is higher than any in the nation. The increase in theft – and also rental car theft – means many of these vehicles are being used to commit crimes. They are often left abandoned, and sometimes they are never recovered. This is a straightforward proposal that will allow the cars to be recovered more quickly, prevent their use in committing crimes, and make sure they are found before they are damaged beyond repair.

3) **Privacy and electronic surveillance technology.** Placed in the state constitution by ballot proposition in 1972, Californians have an inalienable right to privacy, which is enforceable against both the government and private parties. Consistent with that right, the Legislature has enacted numerous policies intended to safeguard individuals' privacy, including the surveillance restrictions this bill seeks to amend. After reports of a Connecticut rental company charging customers extra for speeding, California became one of only a handful of states to restrict the practice of using electronic surveillance technology in rental cars.¹

AB 2840 (Corbett; Chap. 317, Stats. 2004) defined "electronic surveillance technology" to mean a technological method or system used to observe, monitor, or collect information, including telematics, GPS, wireless technology, or location-based technologies, and recognized that despite electronic surveillance technology's utility to the entities employing it and the populations being surveilled, such technology also may violate an individual's right to privacy. Since 2004, concerns about protecting the privacy of Californians have grown significantly in an age where the use of surveillance technology has increased at lightning speed.

¹ See AB 2840 (Corbett, Chap. 317, Stats. 2004).

Since 2012, when General Motors' OnStar debuted Family Link, a service that allowed remote users to track their family members and receive alerts about where the car goes, this type of remote vehicle location technology has become more sophisticated and common with most new cars offering remote vehicle technology that allows someone with a smart phone app to check a car's location, including following the movement of the car in real time; track the history of where the car has been driven; lock and unlock the vehicle remotely; turn it on or off; set the car's climate controls; make the horn honk; and turn on its lights.²

In addition to the remote tracking technology used by consumers, vehicles now often contain exterior and interior cameras that can be used to gather information on drivers. In-vehicle cameras serve a variety of functions, ranging from using facial-recognition technology to automatically adjust seat and mirror settings for each driver, to detecting drowsy or distracted drivers and either alerting them or capping vehicle speed. In the United States, all new cars are required to have backup cameras to help drivers avoid accidents, and other countries have already expanded such safety requirements to include in-vehicle, driver-directed sensors and cameras. However, little is known about how data collected by these cameras is stored and used. Meanwhile, most new cars sold in the United States, including all new Fords, GMs, and BMWs, and nearly all Toyotas and Volkswagens, come with built-in internet connections.

Along with this surveillance technology, smartphones that track virtually every movement of their users, both online and in the real world, have become nearly universal. Vehicles as well, have become computers on wheels along with driver assistance systems, large display screens, internet connections, a multitude of ways to sync smartphones, and contain as many as 200 sensors for collecting data. All of this data is being collected, stored, shared, used, and sold by auto manufacturers and third-party vendors.

For almost 20 years, experts have been warning us about the erosion of our private lives. They note that this erosion is happening one small bit at a time, likely without people even noticing. With the advent of the internet and advances in technology, it is no longer easy for people to decide which aspects of their lives should be publicly disclosed. As Alex Preston noted in *The Guardian* a decade ago:

We have come to the end of privacy; our private lives, as our grandparents would have recognised them, have been winnowed away to the realm of the shameful and secret. . . . Insidiously, through small concessions that only mounted up over time, we have signed away rights and privileges that other generations fought for, undermining the very cornerstones of our personalities in the process. While outposts of civilisation fight pyrrhic battles, unplugging themselves from the web. . . the rest of us have come to accept that the majority of our social, financial and even sexual interactions take place over the internet and that someone, somewhere, whether state, press or corporation, is watching.³

Since this piece was published, it has become increasingly clear that not only is our right to privacy significantly eroded, but our private information and activities are now being harvested and sold for a profit. This commodification of personal information has been dubbed

² Hill, Kashmir. "Your Car Is Tracking You. Abusive Partners May Be, Too." *The New York Times* (Dec. 31, 2023) available at <https://www.nytimes.com/2023/12/31/technology/car-trackers-gps-abuse.html>.

³ Preston, Alex. "The death of privacy." *The Guardian* (Aug. 3, 2014) available at <https://www.theguardian.com/world/2014/aug/03/internet-death-privacy-google-facebook-alex-preston>.

“surveillance capitalism” by social psychologist, Shoshana Zuboff. In an opinion piece for *The New York Times*, in 2021, Dr. Zuboff warned:

As we move into the third decade of the 21st century, surveillance capitalism is the dominant economic institution of our time. In the absence of countervailing law, this system successfully mediates nearly every aspect of human engagement with digital information. The promise of the surveillance dividend now draws surveillance economics into the “normal” economy, from insurance, retail, banking and finance to agriculture, automobiles, education, health care and more. . . .

An economic order founded on the secret massive-scale extraction of human data assumes the destruction of privacy as a nonnegotiable condition of its business operations. With privacy out of the way, ill-gotten human data are concentrated within private corporations, where they are claimed as corporate assets to be deployed at will.⁴

4) **Amendments.** The bill currently in print goes beyond allowing rental car companies to activate surveillance technology faster to locate rental cars when they are not returned on time: it would also allow rental car companies to freely use surveillance technology to collect information on their customers for any purpose, so long as the company included a notice in the rental agreement. Not only would that undermine decades of privacy protections for car rental customers, in the current political environment where many states are moving to criminalize those travelling to seek reproductive and gender affirming care, it could have unintentionally put people in real danger.

The California’s Supreme Court held in 1969 that the state constitution’s implied right to privacy extends to an individual’s decision about whether or not to have an abortion.⁵ This was the first time an individual’s right to abortion was upheld in a court. In 1972, the California voters passed a constitutional amendment that explicitly provided for the right to privacy in the state constitution.⁶ Further, California statutory law provides, under the Reproductive Privacy Act, that the Legislature finds and declares every individual possesses a fundamental right of privacy with respect to personal reproductive decisions, which entails the right to make and effectuate decisions about all matters relating to pregnancy; therefore, it is the public policy of the State of California that every individual has the fundamental right to choose or refuse birth control, and every individual has the fundamental right to choose to bear a child or to choose to obtain an abortion.⁷

With the fall of *Roe v. Wade*, a significant number of states moved quickly to restrict abortions and punish those who are suspected of having them or helping people obtain them. Given these actions whether within the state or in traveling to another state, taking additional steps to secure personal information related to a person’s reproductive health that could conceivably be used as evidence that someone has received that care is of the utmost importance. In fact, one of the recommendations that organizations working to protect people seeking this care is to leave their own car at home and rent a car instead. Arguably, one of the first places that law enforcement

⁴ Zuboff, Shoshana. “You Are the Object of a Secret Extraction Operation.” *The New York Times* (Nov. 12, 2021) available at <https://www.nytimes.com/2021/11/12/opinion/facebook-privacy.html>.

⁵ *People v. Belous* (1969) 71 Cal. 2d 954.

⁶ Prop. 11, Nov. 7, 1972 gen. elec.

⁷ Health & Saf. Code § 123462.

agencies in other states would look to find evidence that someone has come to California to obtain care is the records kept by car rental companies.

Allowing rental car companies to use surveillance technology to collect additional information on their customers at this time would be contrary to California's commitment to being a reproductive freedom state and to this Committee's policy priorities. In particular, such changes could undermine goals of ensuring that all Californians, and those coming from out of state, are protected from punitive, discriminatory, and draconian laws criminalizing people seeking abortion and attacking the LGBTQ+ community's access to essential services such as gender affirming care.

As Oakland Privacy puts it in their letter of opposition to the bill currently in print:

AB 2741 would add a broad exemption that applies to any use imaginable as long as the particular purpose or purposes is disclosed in a terms and conditions disclosure at the time of rental.

There is no reason given for this huge expansion of surveillance use on the part of rental car companies, no limits on the purposes for which the information could be used, and no meaningful disclosure – as in addition to the broad use exemption, the bill also seeks to streamline notification procedures.

Undermining such protections is certainly not the author's goal. Therefore, the author has agreed to remove the broad exemption to the current restrictions on the use of surveillance technology. Specifically, the amendment deletes the following language in section two of the bill:

1939.23(a)(3) The rental company discloses a particular purpose for its collection, access, or use of information relating to the renter's use of the rental vehicle using electronic surveillance technology in the rental or lease agreement or membership agreement.

In addition, in order to continue the consumer protections contained in the current law, suggested Committee amendments restore the requirement that a company notify their customer by telephone and electronically 24 hours before activating the surveillance technology.

So amended, the bill's principal provisions would reduce the waiting period for utilizing surveillance technology for missing rental cars and remove the sunset placed on that exemption. Both changes appear reasonable. As discussed in detail above, with the rapid proliferation of surveillance technology and the myriad of ways that vehicles and other devices are already tracking people, including those using rental cars, it seems unnecessarily restrictive to continue to require a three-day waiting period for these particular businesses.

5) Larger policy questions. While the Committee amendments remove the provision that would have allowed rental car companies to use surveillance technology to collect detailed information on the movements of their customers, as with a number of other bills the Committee has heard this year, the bill raises larger policy considerations related to the invasive nature of technology. Such issues would benefit from additional attention. With the proliferation of surveillance and tracking technology, including built-in vehicle location technology, tracking devices that can easily be concealed in a car or in someone's belongings, in home and public surveillance cameras, automated license plate recognition tools, not to mention the ability to track someone using the smartphones that are virtually universal, at what point has surveillance gone too far?

Should Californians simply accept the complete loss of privacy as people move through their lives in public and private spaces?

Much like the focus that is being placed on the impact of social media, advancement in artificial technology, and the collection and sale of personal information for profit, constant surveillance by private individuals, businesses, and government has a profound impact on Californians' lives. Rather than considering the risks of one device or technological advancement at a time, at some point, it might behoove the Legislature, and this Committee in particular, to explore the larger surveillance policy questions, including the dangers associated with the unchecked proliferation of surveillance tools and their impact on Californians' privacy rights.

6) **Related legislation.** AB 2620 (Ting; Chap. 344, Stats. 2018) allowed rental car companies to use, access, or obtain information relating to a renter's use of a rental vehicle using electronic surveillance technology when the vehicle has not been returned following 72 hours after the contracted return date or the end of any extension, as specified.

AB 1185 (O'Donnell; 2017) would have revised provisions relating to rental company membership programs, advertising, and disclosures. This bill died in the Senate Judiciary Committee.

AB 2051 (O'Donnell; Ch. 183, Stats. 2016), reorganized and reconciled several Civil Code sections addressing rental cars and rental car facilities. The bill provided that entities outside rental companies that rent vehicles provide disclosures to the consumer about customer charges.

AB 675 (Alejo; Ch. 333, Stats 2015), revised and recast the statute governing agreements between rental car companies and their customers in order to allow a rental car company to better separate rental fees from government-imposed charges.

AB 2840 (Corbett; Chap. 317, Stats. 2004) prohibited a rental car company from using, accessing, or obtaining any information relating to a renter's use of the vehicle that was obtained using "electronic surveillance technology," except under specified circumstances.

AB 213 (Leslie; Chap. 427, Stats. 2003) provided that a manufacturer of a new motor vehicle sold or leased in this state that is equipped with one or more recording devices commonly referred to as "event data recorders" or "sensing and diagnostic modules," shall disclose that fact in the owner's manual for the vehicle.

ARGUMENTS IN SUPPORT

Writing in support of the bill, the American Car Rental Association states:

When a vehicle is not returned to the car rental operator at the designated date and time pursuant to the rental contract, the rental company cannot take appropriate steps to locate the asset for 72 hours. One can imagine how far a vehicle could travel or the activities that may occur when criminals are able to procure a means of transportation for the low cost of a rental day and are given a three-day grace period to remain undetected. This significantly increases the risk of the vehicle being lost, vandalized, damaged beyond repair, or used in the furtherance of multiple crimes. Vehicles are frequently found across nearby borders or abandoned and unfortunately, long after a crime has occurred.

The association further notes:

Allowing rental car companies to remotely locate a vehicle after the vehicle is due and when the renter is non-responsive is a reasonable and common sense approach to allowing car rental companies to protect and recover their assets, while also limiting the possibility that stolen rental cars may be used in the commission of additional crimes.

REGISTERED SUPPORT / OPPOSITION:

Support

American Car Rental Association (ACRA)
California Travel Association (CALTRAVEL)

Opposition

Oakland Privacy

Analysis Prepared by: Julie Salley / P. & C.P. / (916) 319-2200